Computer Science
and
Information Systems

Special Edition: Computer Security

Rekenaarwetenskap
en
Inligtingstelsels
The South African Computer Journal
An official publication of the Computer Society of South Africa and the South African Institute of Computer Scientists

Die Suid-Afrikaanse Rekenaartydskrif
'n Amptelike publikasie van die Rekenaarvereniging van Suid-Afrika en die Suid-Afrikaanse Instituut vir Rekenaarwetenskaplikes

Editor
Professor Derrick G Kourie
Department of Computer Science
University of Pretoria
Hatfield 0083
Email: dkourie@dos-lan.cs.up.ac.za

Subeditor: Information Systems
Prof Lucas Introna
Department of Informatics
University of Pretoria
Hatfield 0083
Email: lintrona@econ.up.ac.za

Production Editor
Dr Riel Smit
Mosaic Software (Pty) Ltd
P.O.Box 23906
Claremont 7735
Email: gds@mosaic.co.za

World-Wide Web: http://www.mosaic.co.za/sacj/

Editorial Board

Professor Judy M Bishop
University of Pretoria, South Africa
jbishop@cs.up.ac.za

Professor Richard J Boland
Case Western Reserve University, USA
boland@spider.cwrv.edu

Professor Ian Cloete
University of Stellenbosch, South Africa
ian@cs.sun.ac.za

Professor Trevor D Crossman
University of Natal, South Africa
crossman@bis.und.ac.za

Professor Donald D Cowan
University of Waterloo, Canada
dcowan@csg.uwaterloo.ca

Professor Jürg Gutknecht
ETH, Zürich, Switzerland
gutknecht@inf.ethz.ch

Professor R Nigel Horspool
University of Victoria, Canada
nigelh@csr.csc.uvic.ca

Professor Fred H Lochovsky
University of Science and Technology, Hong Kong
fred@cs.ust.hk

Professor Kalle Lyytinen
University of Jyväskylä, Finland
kalle@cs.jyu.fi

Doctor Jonathan Miller
University of Cape Town, South Africa
jmiller@gsb2.uct.ac.za

Professor Mary L Soffa
University of Pittsburgh, USA
soffa@cs.pitt.edu

Professor Basie H von Solms
Rand Afrikaanse Universiteit, South Africa
basie@rkw.rau.ac.za

Subscriptions

An additional $15 per year is charged for airmail outside Southern Africa

to be sent to:
Computer Society of South Africa
Box 1714 Halfway House 1685
Guest Editorial

Information Security – The Family Member Who Came Home

Basie von Solms
Rand Afrikaans University, Johannesburg, South Africa
basie@rkw.rau.ac.za

The claim that the information society is upon us and that the information superhighway is about to affect us all, is such a cliche that it hardly bears repeating - practically everyone is talking and writing about it. Although the assertion that information security is an essential and integral part of the information society might also seem cliched to some, it nevertheless does not get as much attention and exposure as it should. Information security has always been seen in the same light as taxes: nobody really wants it, but everybody (reluctantly) admits that we need it. Following an alternative analogy, it is like an unwanted family member: we realise that he is part of the family, but we really do not want to be bothered by him. In the last few years, the growth of the Internet and the explosive appearance of the World Wide Web (WWW) has brought information security into corporate boardrooms and private lounges. Suddenly everyone wants to get to know this unwanted family member a little better!

This issue of SACJ is dedicated to the unwanted family member and if, by reading this issue, all of us in the IT family are able to learn just a little more about this sibling, then producing the issue would have been worthwhile. In fact, we should welcome him back home as soon as possible.

A little background about this issue is in order. The International Federation for Information Processing (IFIP) is a consortium of about 60 member countries. It provides an umbrella for many international IT activities. Countries are represented by their national IT society, South Africa being represented by the Computer Society of South Africa (CSSA). IFIP has a total of 13 Technical Committees (TCs), each concentrating on a different aspect of IT. TC 11 deals with all aspects of information security. It organises an annual international conference - the so-called IFIP/Sec series, which is widely regarded as one of the major information security conferences.

IFIP/Sec 95, the 11th International Conference on Information Security, took place in Cape Town in May 1995 and IFIP/Sec 96, the 12th International Conference on Information Security, took place on the Greek island of Samos in May 1996. Complete proceedings of the two conferences, together containing more than 80 articles, have been published by the official IFIP publishers, Chapman and Hall. This issue of SACJ consists of a selection of four articles from the IFIP/Sec 95 Proceedings and two from the IFIP/Sec 96 Proceedings. It is intended not only to disseminate relevant information, but also to bring the information security interests of SAICSIT, CSSA, IFIP and TC 11 to the attention of readers. If, after reading this issue, you are interested in the remaining 74 articles, or in the activities of any of these bodies, please feel free to contact the guest editor directly.

The selected articles cover a diverse range of information security issues. Parker extends its theoretical and conceptual understanding, Hoffman addresses several of its non-technical but crucial aspects, Muflic concentrates on its role in open distributed systems, de Ru and Eloff link into the use of biometrics in information security, von Solms investigates the security protocols for the Internet and WWW, and Pangalos and Khair remind us that information security requirements extend even into the medical field.

The first four articles are from the IFIP/Sec 95 Proceedings. The first, by Donn Parker, suggests a framework for information security in order to avoid information anarchy. He argues that the traditional view of the role of information security - to protect the three elements of confidentiality, integrity and availability of information - is dangerously oversimplified. He includes three more elements of information into the equation: authenticity, utility and possession. The article provides a good platform for gaining a better understanding of what information security really ought to be about.

In the second article, Lance Hoffman addresses the important issues of escrow encryption and export controls - specifically, as he clearly points out, from a US standpoint. The article highlights the very important fact that cryptography is not merely a technical issue, but that the political overtones, civil liberties and administrative implications are also extremely relevant. Ignoring these non-technical issues, as many information security specialists tend to do, will have a negative impact on the field becoming a discipline in its own right. Since its first publication, some of the issues raised by the Hoffman article have been receiving attention. For example, the idea of international cryptography policies is being addressed by the European Organisation for Economic Cooperation and Development (OECD). Relevant recent articles on the escrow aspect can be found in [1].
In the next article, Sead Muftic concentrates on aspects of security in open distributed environments. He identifies a number of elements suitable for a secure system in such an environment. These are: smart cards, secure user workstations, integrated security clients, security servers and a global certification system for international networks. This last aspect is becoming more and more important as basically all secure protocols use public key encryption in some form or the other. Using these elements, he also describes a number of security enhanced applications – secure Internet e-mail and secure EDI. Muftic stresses the fact that all these elements are operational, implemented, and already in use.

de Ru and Eloff then discuss the reinforcement of password authentication, using typing biometrics. Biometric methods are probably the best means of authentication, but many of these methods are technology-intensive and expensive. Their article tries to use typing characteristics as a cheap and user-transparent way to augment the traditional password.

The last two articles are from the IFIP/Sec 96 Proceedings. von Solm's article gives an overview of two non-payment related and one payment related secure protocol for the Internet and the WWW. The non-payment related protocols are Secure Sockets Layer (SSL) and Secure HyperText Transport Protocol (SHTTP). SSL is usable in any TCP/IP environment, while SHTTP is specifically for the WWW. Both make use of public key encryption. The payment related protocol, Secure Payment Protocol (SEPP) was superseded by the Secure Transaction Protocol (SET) early in 1996, but only after the article had already been submitted to IFIP/Sec 96. The presentation at the conference however, covered SET and not SEPP. An appendix is attached to this article, giving a brief overview of SET, as SEPP is no longer relevant. SET also uses public key encryption.

The last article by Pangalos and Khair introduces a methodology to improve the security of medical databases in relation to authentication. Though the methodology of the authors is in itself important and interesting, the article was selected for this issue to underline the importance and relevance of information security in medical IT applications – an area where security introduces new problems quite distinct from those traditionally encountered in the financial and other fields. Because of the differences, information security in medical applications still requires much research.

It is hoped that readers will find this issue of SACJ useful, and also that they will get involved with the activities of the bodies mentioned above.

References


Appendix A

Secure Electronic Protocol (SET) [2] is the secure payment protocol announced by MasterCard and Visa in February 1996. The two previous protocols, SEPP and STI, announced independently by these two companies, were replaced by SET.

This Appendix gives a brief and oversimplified overview of the SET message flow between the customer and the merchant when a payment is made.

Only the most basic parts of messages are discussed, and many details are left out for the sake of simplicity.

The electronic purchasing process can basically be divided into two phases. Phase 1 is a browsing and negotiation phase in which the customer will decide what to buy. Goods and price will be negotiated and agreed upon between the customer and merchant. The phase will probably end with a completed order form, specifying the goods, with the associated price, the customer is about to buy.

At this point the customer decides to start Phase 2, the payment phase. It is at this point that the SET payment protocol is initiated.

Step 1:
A message is sent from the customer to the merchant, requesting, amongst other things, the public key certificates of the merchant and the merchant's acquirer.

Step 2:
The merchant sends these certificates back to the customer.

Step 3:
- The customer validates the certificates received from the merchant.
- The customer constructs the Order Information (OI).
- The customer generates a DES key K1 and encrypts OI under K1, giving K1(OI).
- The customer encrypts K1 using the public key of the merchant, giving MP(K1).
- The customer constructs the hash of the OI, giving H(OI).
- The customer constructs the Payment Information (PI). The PI contains info about the credit card nr, expiry date etc.
- The customer generates a DES key K2 and encrypts PI under K2, giving K2(PI).
- The customer encrypts K2 using the public key of the acquirer, giving AP(K2).
- The customer constructs the hash of the PI, giving H(PI).
- The customer constructs the hash of OI, the hash of PI and concatenates them, giving H(OI)||H(PI).
- The customer digitally signs this concatenation giving S(H(OI)||H(PI)). The customer performs...
Step 4:  
The customer sends the message $M_1 = [K_1(OI), MP(K_1), H(OI), K_2(PI), AP(K_2), H(PI), S(H(OI)||H(PI))]$ to the merchant.

Step 5:  
The merchant receives $M_1 = [K_1(OI), MP(K_1), H(OI), K_2(PI), AP(K_2), H(PI), S(H(OI)||H(PI))]$
- The merchant retrieves $K_1$ and then $OI$.  
  Note that the merchant cannot retrieve $PI$ in any way. The customer intended it this way, because he/she does not want the merchant to see his credit card info.
- The merchant creates $H(OI)$, concatenates it with $H(PI)$ received in $M_1$, and compares it with the $H(OI)||H(PI)$ received in $M_1$.  
  Note that the merchant can retrieve $H(OI)||H(PI)$ from $S(H(OI)||H(PI))$ by using the customer's public key.  
  If they are equal, then the merchant knows that the $OI$ he/she has retrieved from $M_1$ is the 'correct' $OI$ intended by the customer to accompany the $PI$ provided by the customer.  
  Note that this process allows the merchant to associate a specific $OI$ with a specific $PI$ without knowing precisely what $PI$ is.

Step 6:  
The merchant now requests an authorisation from his acquirer, by sending the following message $M_2$ to the acquirer: $[H(OI), K_2(PI), AP(K_2), H(PI), S(H(OI)||H(PI))]$
- The acquirer goes vica versa through the same procedure as the merchant, allowing the acquirer to associate the specific $PI$ with the specific $OI$ without knowing precisely what $OI$ is.  
  The customer does not want the acquirer to see what he/she is buying, but wants the acquirer to link the $OI$ to the $PI$.

Step 7:  
If necessary, the acquirer gets authorisation from the issuer, and send a digitally signed authorisation back to the merchant.

Step 8:  
The merchant informs the customer that the transaction is authorised.
Encryption Policy for the Global Information Infrastructure*

Lance J Hoffman
Institute for Computer and Telecommunications Systems Policy and Department of Electrical Engineering and Computer Science, The George Washington University, Washington, D.C. 20052 USA
hoffman@seas.gwu.edu

Abstract

Cryptology policy deals not only with various technological encryption methods but also with thorny political and administrative problems. It is a challenge to address these in a timely and open manner. The problems arise in law enforcement, civil liberties, and export control policy. They must be confronted if a rational cryptographic policy is to provide a framework in which technological solutions can operate.

Keywords: Information Security, Cryptology Policy, Export Control
Computing Review Categories: D.4.6, K.4.2, K.4.1

1 Introduction

The announcement of the Clipper chip by the U.S. Government in April 1993 set off a frenzy of discussions about cryptography policy in the computer community. The shock waves from it ultimately produced front page treatment in The New York Times, repeated questions to the Vice President of the United States, and a new newsgroup on the Internet. They also produced a great deal of public discussion about striking the balance between national security, law enforcement, and civil liberties.

As the Global Information Infrastructure develops, more governments are becoming concerned with communications privacy and security. This is not a new phenomenon; even before the French revolution governments were worried about accountability of authors and publication of seditious materials [22]. In 1993, the scepter of effectively unbreakable cryptography available to any individual pushed the United States government into launching three interrelated initiatives: the digital telephony improvement initiative, the Clipper chip key escrow encryption initiative, and export control reform. The first effectively makes the public switched telephone network "wiretap-friendly"; the second promotes encryption that can be broken, under certain conditions, by the government; the third is supposed to expedite licensing of encryption product exports.

We attempt here to present a survey of the policy issues in a non-ethnocentric manner. However, since the United States has been in the forefront of framing the debate, and since the author has been close to that debate, this account necessarily will reflect his knowledge. It would be welcome if similar accounts from other countries were made available.

This paper does not examine the technology of cryptography; readers interested in those issues are referred to [2, 5, 37, 25, 14]. Here, we present a Cook's Tour of encryption policy, sketching out the general landscape and providing pointers on where to go to get more detailed information.

The Digital Telephony Initiative

The digital telephony initiative was a successful effort by the U.S. Government to maintain some capability to wiretap in cases where advances in telecommunications technology could (or had already) outrun law enforcement's ability to intercept communications in order to enforce laws and protect national security. Recent legislation [24] passed by the U.S. Congress requires telecommunications carriers to ensure that they possess the capability and capacity to enable the government to isolate and intercept, pursuant to authorization by a court, call identifying information and the contents of a communication. The requirements apply only to carriers who engage in "the transmission of switching of wire or electronic communications as a common carrier for hire." They do not apply to information service providers (the Internet, America Online, Prodigy, etc.), to private networks, or to PBX's. The requirements for obtaining a warrant prior to the interception have not been changed. Law enforcement cannot require a carrier to install a port which can be remotely activated by a law enforcement officer. All taps must be conducted with the intervention of the carrier (as is the case under current law).

The new law authorizes US$500 million to be paid by the government for this retrofitting of the telephone system.

The Clipper Chip Key Escrow Encryption Initiative

The key escrow encryption initiative (popularly known as the "Clipper plan", or just "Clipper") is a U.S. Government attempt to protect communications against industrial espionage and other compromises while at the same time maintaining the existing capability of law enforcement and national security agencies to eavesdrop, with a court order, on suspect communications. When law enforcement or national security agencies are interested in a person's
communication, they obtain a warrant from the appropriate issuing authority. They then fax a notification that they have this to two independent government agencies (currently the National Institute of Standards and Technology and the Automated Systems Division of the Department of the Treasury), who then each give up half of the digital key necessary to decrypt the conversation. When the two half-keys are joined to form the entire key, law enforcement officials can then obtain the unit key for the given chip used in the communicating telephone and use it to decrypt the conversation (assuming that telephone has used the Clipper chip in the first place). A detailed description of the system appears in [11].

This so-called "escrowed encryption standard" [34] is encouraged but voluntary in the federal government. The Administration, after looking into potential violations of the U. S. Constitution, decided not to make it mandatory for private persons. Nevertheless, it clearly hopes that almost everybody will use this system. Some civil libertarians and outside observers are concerned that it will become mandatory in the future. Indeed, FBI Director Louis Freeh has been quoted as stating that he will have to seriously consider proposing this if public acceptance of Clipper does not increase.

No one has seriously suggested that the algorithm is insecure (although a method of using it which negates any value to law enforcement because of a minor design flaw (now being corrected) made the front page of The New York Times on June 2, 1994). But many do not completely trust the key escrow agents. Many suggestions have been made such as adding a third escrow agent from the private sector, or one from the judicial branch of government, or letting users pick whichever escrow agents they want, or having software manufacturers serve as the escrow agents, etc. Only recently has the government started seriously looking at some of these alternatives, possibly due to the cold reception generally accorded Clipper.

Clipper's encryption algorithm, "Skipjack", fits into Capstone, the U.S. government's long-term project to develop a set of standards for publicly available cryptography for use in voice and data communications. In one scenario, the government itself and all private companies doing electronic business with the government would be required to use Capstone, which could all be contained on a single computer chip. This would provide economies of scale but would also force users who wanted "government-proof" communications to superencrypt using other commercially available algorithms.

Export Control Reform

There is a large and growing collection of encryption software and hardware available around the world (see Figure 1). The October 1994 Software Publishers Association Foreign Availability Study turned up 870 products in 24 countries, 394 products of which are manufactured outside the United States [39]; roughly half of these use DES. Since with export controls, sales may be (and have been [41]) lost to non-U.S. competitors with stronger encryption packages, one U.S. vendor has actually set up a completely independent cryptographic development lab overseas, from which crypto products can be exported almost anywhere, including the United States.

Only recently have export controls been loosened a bit so traveling business executives can at least take their laptops overseas and encrypt information using the Data Encryption Standard [31] without violating the export laws (in theory - for a first-hand account of what actually happens when one tries to comply with this U.S. law, see [4]). There is some Congressional interest in abandoning many export controls on encryption, arguing that the economic needs outweigh the national security needs. The U.S. Commerce Department is currently studying this issue. They appear to be convinced of the foreign availability of strong (DES or "better") encryption, but are looking into how badly its nonexportability harms U.S. firms.
2 Key Escrow Cryptosystems

Key escrow systems are those where part or all of the cryptographic keys are kept "in escrow" by third parties. The keys are released only upon proper authority to allow some person other than the original sender or receiver to read the message. The U.S. government is strongly supporting key escrow as a way to balance the needs for secrecy between communicating persons against the needs of law enforcement and national security agencies to sometimes read these encrypted communications (with proper legal authority).

U.S. Government Key Escrow

As of this writing, the U.S. Government's initial and only key escrowing suggestion is the Escrowed Encryption Standard [34] which defines a family of processors popularly known as Clipper chips. It uses the Skipjack algorithm which is classified but has been examined by a non-Government review team; this team had only a limited time to consider brute force attacks by exhaustive search, susceptibility to shortcut attacks, and the National Security Agency's design and evaluation process. Their interim report, the closest thing to a technical evaluation publicly available, concluded that [7]:

1. Under an assumption that the cost of processing power is halved every eighteen months, it will be 36 years before the cost of breaking SKIPJACK by exhaustive search will be equal to the cost of breaking the Data Encryption Standard today. Thus, there is no significant risk that SKIPJACK will be broken by exhaustive search in the next 30-40 years.
2. There is no significant risk that SKIPJACK can be broken through a shortcut method of attack.
3. While the internal structure of SKIPJACK must be classified in order to protect law enforcement and national security objectives, the strength of SKIPJACK against a cryptanalytic attack does not depend on the secrecy of the algorithm.

After this report was issued, Blaze described potential problems with Clipper that this review team failed to mention [3], including two methods to avoid message interception by the government. While there are more effective ways of "beating the system" (like superencryption) which are well-known, this paper made front page news in the New York Times [28], sending shock waves across some policymakers' radar screens.

The U.S. Government hopes that the Capstone chip, which incorporates several government standards including Skipjack, will be widely used in both public and private sectors. It is being installed in "Fortezza" PCMCIA electronic boards and used for the Pre-message Security Protocol (PMSP) program for the security of the Defense Messaging System. It implements the Skipjack algorithm (for bulk data encryption), the digital signature algorithm as specified in the digital signature standard [33], a key exchange algorithm based on a public key exchange, and the secure hashing algorithm (NIST 1994c).

On July 20, 1994, Vice President Gore acknowledged some of the problems with Clipper and stated that "the Clipper chip is an approved federal standard for telephone communication and not for computer networks and video networks"; that he would like a "more versatile, less expensive system" with "key escrow implementable in software, firmware or hardware, or any combination thereof" which "would not rely on a classified algorithm"; and that "there are many severe challenges to developing such a system" which "must permit the use of private-sector key escrow agents as one option". He promised [18] to reassess the current relatively strict export control licensing regime based on the results of two government studies to be carried out in 1994 and 1995.

Alternatives

There are alternatives to Government Key Escrow. Micali has patented a process [29] for building a "fair" cryptosystem that balances the needs of the Government and those of the public and private sectors. It appears to cover the Escrowed Encryption Standard (Clipper) and the U.S. government has negotiated with him a limited use license for state and federal law enforcement. Banker's Trust International has proposed a common key escrow system for government and commerce using unclassified algorithms, with users having public-private keys [38]. Trusted Information Systems [1] has proposed two software-only designs for key escrow systems, one paralleling Clipper and one an improvement which is likely to be much more palatable to private organization [42]. The latter (see Table 1) is really more properly called a (near-) real-time emergency access system, since there is nothing in escrow and no escrow agent. The U.S. Government itself is actively examining alternatives [32]. These generally avoid some of the practical problems associated with the official U.S. Government key escrow system [12].

3 Law Enforcement and Civil Liberties Issues

Some assert [10] that the Clipper Chip initiative strikes the proper balance between individual and organizational needs for secret communications with our common need for public safety and monitoring of criminal and terrorist activities. Civilized life is a compromise and everything has honest costs [17]. But people disagree on these "honest costs". While most expert testimony submitted to the government opposed both Clipper and current export controls and while the public comments by organizations and individuals were 318-2 against the initiative [27], the government decided that the arguments on the other side were more compelling; it never issued the report on Clipper it promised when announcing the initiative in April 1993.

This ongoing communications gap and lack of trust between the federal government (especially the national security agencies with their closed culture) and much of the computer community and the media poisoned the Clipper
Table 1. (Near) Real-time emergency systems

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Clipper</th>
<th>Micali</th>
<th>TIS “Commercial Key Escrow”</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of escrow agents</td>
<td>2</td>
<td>no</td>
<td>none</td>
</tr>
<tr>
<td>Defined agents</td>
<td>Government (Administrator)</td>
<td>Don’t care</td>
<td>Corporate, government, or private data recovery center</td>
</tr>
<tr>
<td>Secure hardware</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Direct cost to end-user</td>
<td>US$25 (eventually)</td>
<td>$0 metered (possibly anonymous) phone calls</td>
<td></td>
</tr>
<tr>
<td>Majority logic (K of N can allow access)</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Can use public key systems</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Allow law enforcement real-time access</td>
<td>yes</td>
<td>It depends</td>
<td>It depends</td>
</tr>
<tr>
<td>Secrets kept at</td>
<td>central site</td>
<td>central site</td>
<td>user machine</td>
</tr>
<tr>
<td>Other properties</td>
<td>???</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

discussions for a long time. Indeed, one local trade publication questioned why the National Security Agency (NSA), supposedly not involved in domestic issues, has taken such an active role in advocating Clipper as a national encryption standard; it effectively stated that “the agency is breaking the law”[6]. But if, as many (especially in the national security community) argue, key escrow systems represent “the last chance to protect personal safety and national security against a developing information anarchy that fosters criminals, terrorists and foreign foes”[27], shouldn’t these and other systems be examined more closely, and by a broader range of people?

In fact, this is what is happening. The debate has now shifted from relatively arcane technological details to the policy matters. A broad policy review is now being carried out by the National Research Council. One important outcome of this should be “the development of more open processes to determine how cryptography will be deployed throughout society in support of electronic delivery of government services, copyright management, and digital commerce”[35]. This report will not be ready until 1996. Walker suggests that is too long a time and that if the problem is not resolved by using “commercial key escrow” as opposed to “government key escrow”, and soon, the opportunity will be lost to limit the expansion of incompatible product-by-product solutions. He thinks that if governments continue to “study the problem”, a plethora of cryptographic mechanisms will be put into computing software, and that this will seriously damage law enforcement and national security interests[42].

Should anyone be able to develop and disseminate encryption technology or should it be “born classified”? Diffie is concerned about the effect of a secret cryptographic standard on individual rights and technology development[13] and on innovation in the computer and communications industries. He states that the public (not government) cryptographic community has been the principal source of innovation in cryptography; he does not want to hobble this innovation. He has urged that all aspects of Clipper be made public, not only to expose them to public scrutiny but also to guarantee that once made available as standards they will not be prematurely withdrawn by an all-powerful agency. He observes that “law, technology, and economics ... must all be kept in harmony if freedom is to be secure” and wants rights (such as that to have a private conversation) recognized by law to be supported rather than undermined by technology.

The American Civil Liberties Union (ACLU), reacting to the announcement of the Clipper Chip proposal, expressed a concern that the rights protected under the First, Fourth, and Fifth Amendments of the U.S. Constitution (freedom of speech; no unreasonable search and seizure, warrants with particulars; no self-incrimination or private property taking) may be violated. They also assert that the present system of export controls on cryptography is unconstitutional, a point apparently agreed with by an assistant attorney general in a 1978 government memo[20].

Froomkin sees the issue as less clear, however. As he points out, “the rights of private non-commercial users appear to be a distressingly close question given the current state of civil rights doctrine and the great importance that the courts give to law enforcement and national security.”[16]

To show that the public welfare may indeed be threatened by too much and too good cryptography available to the general public, we present an example of the criminal sophistication that is possible with today’s technology: the undetectable electronic crime. This is provided in a mathematical formulation in about a page by[40]. The reader, and the populace, will have to judge whether the scepter of enough of these is so likely and so threatening that diminution of some other civil liberties is warranted.

Because of these concerns, a bill (H.R. 5199) was introduced in the 1994 U.S. Congress to regulate “voluntary
encryption standards" for privacy, security, and authenticity of domestic and international electronic communications. Its key features include:

- The Secretary of Commerce will establish an Encryption Standards and Procedures Program conducted by the director of the National Institute of Standards and Technology. The Secretary will be authorized to conduct research, make grants, and enter into agreements.
- Any encryption standard put forward by the Secretary shall meet the following requirements: ensure confidentiality, integrity, or authenticity of electronic communications; advance the development of the National Information Infrastructure (NII); contribute to public safety and national security; preserve existing privacy rights; preserve the functional ability of government to interpret electronic information lawfully obtained; be implementable in software, firmware, or hardware.
- Standards shall be developed in consultation with the Attorney General, the Federal Bureau of Investigation, the National Security Agency, and other federal agencies. The Computer System Security and Privacy Advisory Board shall review any standard before issuance.
- Nothing in [this act] shall be construed to require the use of such standards.
- Key escrow agents may be established by the President. Each escrow agent will be a federal agency that is competent to administer the program and is not a federal agency authorized by law to conduct electronic surveillance.
- The key escrow agent may only disclose the keys to an authorized government entity and that entity may only use the keys for the purpose expressly provided for in the court order. Foreign entities may have access to the keys if the President determines that it would be in the national security interests of the United States.
- The Secretary of Commerce shall conduct a public hearing every three years on the program and then submit a report to Congress.

The Electronic Privacy Information Center of Washington welcomed this first attempt to "bring encryption standards setting under the rule of law", but proposed several standards that the FBI, NSA, and the Attorney General have proposed that the FBI, NSA, and the Attorney General have implemented.

4 Export Policy: Prudent Controls in a Risky World?

The United States Government continues to impose rigid controls on the export of encryption software and hardware products, despite evidence that the policies governing the issuing of export licenses inhibit U.S. businesses' ability to compete in the foreign marketplace — a marketplace that already offers encryption software and hardware that incorporates the very standards that U.S. businesses cannot export because of export controls.

Exports of cryptographic software and hardware are controlled by the U.S. Department of State and the U.S. Department of Commerce. The State Department uses the International Traffic in Arms Regulations (ITAR) which include the "Munitions List"; this list enumerates munitions material for which export licensing is required; encryption materials are included in Category XIII. Commerce Department requirements are set forth in the Export Administration Regulations and the Commerce Control List. The National Security Agency (NSA) has a very strong voice in these decisions.

Walker [41] describes importing several DES products and notes the "frustrating and somewhat humorous" incident in which NIST posted source code for DES to the Internet without an export restriction notice and it was immediately copied by computers in Denmark, the United Kingdom, and Taiwan. As he points out, FIPS 181 (which contains the DES source code) now "is available from hosts throughout the world along with the notice that export from the U.S. is in violation of U.S. export controls."

Complying with export regulations is daunting, and a manufacturer who is exporting software or having foreign nationals develop it could unwittingly run afoul of U.S. law [9] That's what may have happened to Phil Zimmermann, the author of Pretty Good Privacy (PGP), who has come under pressure from the U.S. government for the unregulated distribution of strong encryption. A federal grand jury in San Jose, California is examining whether he broke laws against exporting encryption codes. He says a friend, who he refuses to identify, put PGP on the Internet. Zimmermann's lawyer says his client could face charges carrying a prison sentence of up to 51 months. [8] Miller, in a fundraising appeal for the Phil Zimmermann Defense Fund posted to a number of newsgroups, claims that the government also hopes to establish the proposition that posting a cryptographic program on a bulletin board system or on the Internet is the same as exporting a "munition" [30].

There are two conflicting U.S. government rulings on the legality of exporting cryptographic information. In the first, the Department of State [21] ruled that export of a diskette with source code for high quality cryptography is prohibited, even though export of the same source code printed in a book is allowed (even in this day of inexpensive scanners!). The second [20] is a Justice Department memorandum to the Science Advisor to the President, stating that "the present ITAR licensing scheme does not meet constitutional standards". This memorandum concluded that "a prepublication review requirement for cryptographic information might meet First Amendment standards if it provided necessary procedural safeguards and precisely drawn guidelines." Apparently, an informal system of prepublication review instituted in 1981 [36] has worked well for the publication of cryptographic papers. A broad-based
committee of the Association for Computing Machinery has written that "As far as the research community has been concerned, it is fair to say that there have been no long-term chilling effects." [26]

Charles A. Hawkins, Jr., Acting Assistant Secretary of Defense (C3I) summarized the encryption policy issue very well in a memo for the U.S. Deputy Secretary of Defense on May 3, 1993. He correctly observed that encryption policy is not a technological issue:

"Trapdoor encryption technology is not essential to the debate since a system that required the escrow of keys by users of cryptographic technologies could be established even if the trapdoor chips did not exist. Proposed use of trapdoor technology does raise a further complication: neither the academic community nor private industry is comfortable with encryption algorithms that are kept secret, as will be the case with the trapdoor chip. It has been suggested that an independent panel of cryptography experts will be invited to evaluate the algorithm. This will not reassure the community at large that there are no unrecognized vulnerabilities, since the panel will be perceived as captive and tainted.

5 Summary

We have clearly learned a lot in the first years of the cryptographic policy debate, and are starting to deal with the thorny technological, political, and administrative issues it raises. It will be a challenge to do this in a timely manner and in an open fashion. We hope that this survey provides a good start in that direction.

References

1. D M Balenson, C M Ellison, S B Lipner, and S T Walker. 'A new approach to software key escrow encryption'. In Hoffman [23].
7. E F Brickell, D E Denning, S T Kent, D P Maher, and W Tuchman. SKIPJACK review: Interim report. Posted to sci.crypt, August 1, 1993 by Dorothy Denning (reprinted in [23]).
16. A M Froomkin. 'The constitutionality of mandatory key escrow – A first look'. In Hoffman [23].
26. S Landau, S Kent, C Brooks, S Charney, D Denning,
32. National Institute of Standards and Technology. 'Opportunity to join a cooperative research and development consortium to develop secure software encryption with integrated cryptographic key escrowing techniques'. Federal Register, Notices, 58(162), (August 24 1993).
Notes for Contributors

The prime purpose of the journal is to publish original research papers in the fields of Computer Science and Information Systems, as well as shorter technical research notes. However, non-refereed review and exploratory articles of interest to the journal’s readers will be considered for publication under sections marked as Communications or Viewpoints. While English is the preferred language of the journal, papers in Afrikaans will also be accepted. Typed manuscripts for review should be submitted in triplicate to the editor.

Form of Manuscript

Manuscripts for review should be prepared according to the following guidelines.

- Use wide margins and 1½ or double spacing.
- The first page should include:
  - title (as brief as possible);
  - author’s initials and surname;
  - author’s affiliation and address;
  - an abstract of less than 200 words;
  - an appropriate keyword list;
  - a list of relevant Computing Review Categories.
- Tables and figures should be numbered and titled.
- References should be listed at the end of the text in alphabetic order of the (first) author’s surname, and should be cited in the text in square brackets [1-3]. References should take the form shown at the end of these notes.

Manuscripts accepted for publication should comply with the above guidelines (except for the spacing requirements), and may be provided in one of the following formats (listed in order of preference):

1. As (a) \LaTeX file(s), either on a diskette, or via e-mail/ftp - a \LaTeX style file is available from the production editor;
2. As an ASCII file accompanied by a hard-copy showing formatting intentions:
   - Tables and figures should be original line drawings/printouts, (not photocopies) on separate sheets of paper, clearly numbered on the back and ready for cutting and pasting. Figure titles should appear in the text where the figures are to be placed.
   - Mathematical and other symbols may be either handwritten or typed. Greek letters and unusual symbols should be identified in the margin, if they are not clear in the text.

   Contact the production editor for markup instructions.
3. In exceptional cases camera-ready format may be accepted – a detailed page specification is available from the production editor;

Authors of accepted papers will be required to sign a copyright transfer form.

Charges

Charges per final page will be levied on papers accepted for publication. They will be scaled to reflect typesetting, reproduction and other costs. Currently, the minimum rate is R30.00 per final page for \LaTeX or camera-ready contributions that require no further attention. The maximum is R120.00 per page (charges include VAT).

These charges may be waived upon request of the author and at the discretion of the editor.

Proofs

Proofs of accepted papers in category 2 above may be sent to the author to ensure that typesetting is correct, and not for addition of new material or major amendments to the text. Corrected proofs should be returned to the production editor within three days.

Note that, in the case of camera-ready submissions, it is the author’s responsibility to ensure that such submissions are error-free. Camera-ready submissions will only be accepted if they are in strict accordance with the detailed guidelines.

Letters and Communications

Letters to the editor are welcomed. They should be signed, and should be limited to less than about 500 words.

Announcements and communications of interest to the readership will be considered for publication in a separate section of the journal. Communications may also reflect minor research contributions. However, such communications will not be refereed and will not be deemed as fully-fledged publications for state subsidy purposes.

Book reviews

Contributions in this regard will be welcomed. Views and opinions expressed in such reviews should, however, be regarded as those of the reviewer alone.

Advertisement

Placement of advertisements at R1000.00 per full page per issue and R500.00 per half page per issue will be considered. These charges exclude specialized production costs which will be borne by the advertiser. Enquiries should be directed to the editor.

References

Contents

GUEST EDITORIAL

Information Security – The Family Member Who Came Home
SH von Solms ................................................................. 1

SPECIAL EDITION: COMPUTER SECURITY

A New Framework for Information Security to Avoid Information Anarchy
DB Parker ................................................................. 4

Encryption Policy for the Global Information Infrastructure
LJ Hoffman ............................................................... 10

Functional and Operational Security System for Open Distributed Environments
S Muftic ................................................................. 17

Reinforcing Password Authentication with Typing Biometrics
WG de Ru and JHP Eloff ............................................... 26

Information Security on the Electronic Superhighway
SH von Solms ............................................................... 36

Design of Secure Medical Database Systems
G Pangalos and M Khair .................................................... 45