RSA
DATA SECURITY, INC.
THE KEYS TO PRIVACY AND AUTHENTICATION

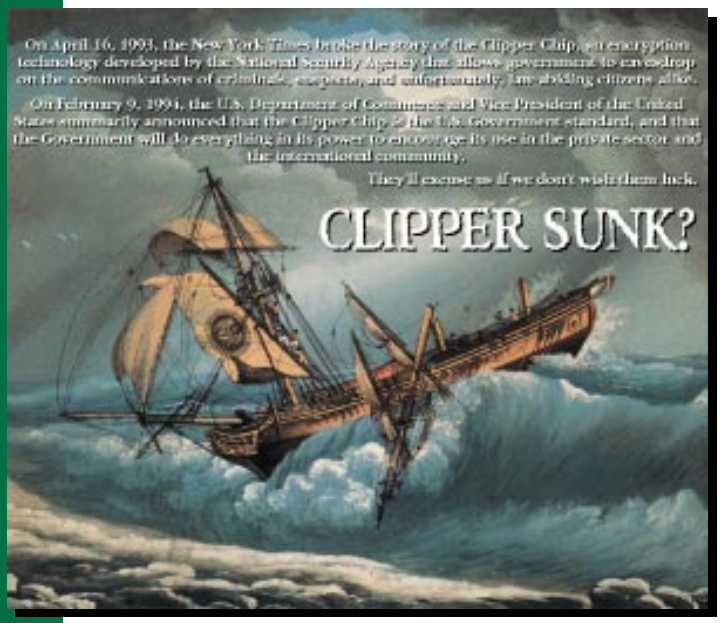
Ciphertext
THE RSA NEWSLETTER

Volume 2, No. 1 Summer 1994

In This Issue:

Did Washington Blink?

In a July 21 letter to Rep. Maria Cantwell of Washington, Vice President Al Gore said that the administration was "willing to explore industry alternatives" to Clipper, the NSA-designed encryption scheme with a built-in mechanism for government "monitoring" of encrypted communications. This is good news, although not a complete sinking of the Clipper initiative. Mr. Gore emphasized throughout his letter a continuing commitment to key escrow encryption, the core of the Clipper initiative.



Perhaps we should release this "revised edition" of our infamous poster...

The overwhelming private industry preference, expressed frequently, continues to be for no key escrow. Despite this, Mr. Gore reiterated the administration's commitment to escrowed encryption and to the use of the Clipper chip in telephones, while announcing over a year of Presidential studies on possible other key escrow systems for data and video. Of course, escrowed encryption is said to be "voluntary" — but corporations have complained that if they want or need to communicate securely with a government agency, they will be cornered into using key escrow.

Crypto Export Restrictions Remain

Despite the introduction of legislation by Rep. Maria Cantwell which would have liberalized export restrictions, VP Gore's let

continued on page 11

1994 RSA Data Security Conference

This year's RSA Data Security Conference was the largest ever, with over forty organizations presenting product and technology announcements, numerous technical presentations, several product demonstrations, and a meeting of the IEEE working group on public-key standards. The conference spanned three days-January 12th through January 14th-and was attended by over 350 people. Here are some highlights.

The most striking aspect of the conference was the variety of companies announcing

continued on page 9

Bruce Heiman on Domestic and Overseas Encryption

We are pleased to reprint an edited transcript of Bruce Heiman's talk at the 1994 RSA Data Security Conference. Mr. Heiman is a graduate of Harvard Law School and a partner in the prestigious Washington law firm of Preston Gates, and is active in the Business Software Alliance, an industry consortium working to eliminate export controls on encryption software.

Bruce Heiman: Coming at the end of a long day like this you sort of feel like Zsa Zsa Gabor's seventh husband! I know what I am supposed to do–I just don't know how to make it interesting.

...At least some of us in the industry are taking the government at its word that in fact Clipper will only be voluntary. But what we have said is, the touch-tone test as to whether or not it will be voluntary is: are we going to be able to freely export other programs and products using other algorithms, using other encryption regimes? That issue has really yet to be fully joined and certainly is yet to be resolved. The promised inner-agency study within the administration continues. It has been delayed time and time again. What will be pushing it now in fact is legislation that was introduced right before Congress left for its recess, a bill in the house introduced by Congressman Maria Cantwell from Washington State, that would significantly liberalize export controls of encryption programs and products. Let me just briefly tell you what that does, and then maybe give you a flavor of the debate that has been going on, principally within NSA and industry and is going to become a much more public debate on the hill since the legislation will be considered as soon as next month.

First, the bill essentially precludes the government from requiring export licenses for generally available software. It used to be referred to as "mass market" (although that is a term of art and is too limited), these days in terms of electronic distribution and CD-ROM, but the stuff that comes in a box, the stuff that comes down the wire, the stuff that is sold for all of the PCs everywhere - you would not need an export license for software, nor would you need an export license for hardware implementations of generally available software.

Second, the bill directs the government to issue export licenses for custom software that is sold as part of a computer system, sale on the same terms and conditions, essentially, that you can now export to financial institutions. That would significantly free up DES implementations.

Over one-third of Fortune 500 companies surveyed specifically look for encryption when purchasing software.

In both cases the bill does not limit the government's ability to restrict exports in the case of terrorist countries or in the case of programs or products that are specifically designed for military applications. Not if they could "possibly, maybe, if they were a little bit altered" be used for military applications but were *specifically* designed for military applications.

Lastly, it puts the entire licensing process over in the Department of Commerce rather than where it is now, which is the State Department, where really NSA is making the decisions.

A potential market of six to nine billion dollars

NSA has not taken well to the legislation and continues to make a number of arguments. I would like to give you the flavor of these.

The first argument is that there is no consumer demand, no user demand for encryption and (audience laughter) you are laughing... I wish it were funny! One of the best answers (to that argument) is ...count them up ... there were 12 companies here today (announcing new RSA-based products). I don't know, my perception is that they wouldn't be investing their time, money and resources in insuring that their products provide security if they were doing it on a whim, or if they though their customers didn't really care about it.

The Business Software Alliance asked Frost and Sullivan to do a market survey of Fortune 500 companies here in the United States as to their security needs. The results I thought were pretty interesting. 90% said that information security was important to their operation; 78% said very important. Interestingly, three-quarters also said that it was important to communicate electronically not only within their own operations but also upstream and downstream with their supplies and with their customers. *Almost half* specifically said that encryption was important and *over one-third* said that they specifically look for encryption when purchasing software . And over one-third said that they would consider buying foreign software if it had information security, if it offered the information security an American product did not...and that translates into a potential market of *six to nine billion dollars.*

...for a long time NSA argued that 'We don't have to worry - there are no foreign programs and products offering encryption capabilities.' Well, the Software Publishers Association, beginning in early 1993 late 1992, started compiling information on the foreign availability of programs and products manufactured abroad. At this point there are well over 200 foreign programs and products that they have found that provide encryption capabilities .... presented with the evidence that there are all these foreign programs and products, NSA now argues they aren't worth much (cryptographically). ...They said 'Well even if you can export them it's not really DES.' We said 'Well, DES is DES, you know. It is standard implementation. You do it, it either works or it doesn't.' They said 'Well, DES implementations are different. Maybe there are weak DES implementations. Well, maybe there are some performance differences but it either works

continued on page 8

New RSA Licensees

Since November 1993 we've had several new addtions to the RSA family. Please join us in welcoming both these new RSA licensees and some new products from our old friends.

ALCATEL TITN
TWICE CDPD

APPLE
System 7.5

BANKERS TRUST
Bankers Trust Authentication Services

CINCINNATI MICROWAVE
MC-DART 100 CDPD wireless modem

DIGITAL DELIVERY
CD Product Portfolio

ENTERPRISE INTEGRATION TECHNOLOGIES
Secure MOSAIC & CommerceNet

ENTERPRISE SOLUTIONS
ES/Secure for X.400 Mail

FUNK SOFTWARE
WanderLink Remote Access

GENERAL MAGIC
Magicap Operating System

HEWLETT PACKARD
Cryptographic Module for HP 9000

HILGRAEVE
HyperACCESS/5

HELPFUL PROGRAMS, INC.
Instalit, hpOMNI

LAN SUPPORT GROUP
Bindview NCS NetSqueeze+Encryption

LOTUS
Lotus Forms

NATIONAL SEMICONDUCTOR
iPower Secure Tokens

NORTHERN TELECOM
Entrust Encryption Software

ORACLE
SQL*Net Secure Client/Server Database

PCSI
Ubiquity 1000

PITNEY BOWES
Veritas ID Authentication Systems

RETIX
ROUTERXchange* RX 7000 MD-IS Router (CDPD)

SPYRUS
Secure CD-ROM

TERISA SYSTEMS
RSA Crypto Toolkits for WWW

TRANSCRYPT INTERNATIONAL
DME 9600 Dual Mode Encryptor

World Wide Web Beefs Up Security with RSA for CommerceNet Market Trial

Enterprise Integration Technologies (EIT), the National Center for Supercomputing Applications (NCSA) and RSA Data Security today announced agreements to jointly develop and distribute a secure version of NCSA Mosaic, the popular point-and-click interface that enables easy access to thousands of multimedia information services on the Internet.

Secure Mosaic will help unleash the commercial potential of the Internet by enabling buyers and sellers to meet spontaneously and transact business.

The announcement was made in conjunction with the launch of CommerceNet, a large-scale market trial of electronic commerce on the Internet. Under the agreements, EIT will integrate its Secure-HTTP software with public key cryptography from RSA into NCSA Mosaic Clients and World Wide Web (WWW) servers. WWW is a general-purpose architecture for information retrieval comprised of thousands of computers and servers that is available to anyone on Internet.

Jay M. Tenenbaum, chief executive officer of EIT, believes secure NCSA Mosaic will help unleash the commercial potential of the Internet by enabling buyers and sellers to meet spontaneously and transact business electronically.

"While NCSA Mosaic makes it possible to browse multimedia catalogs, view product videos, and fill out order forms, there is currently no commercially safe way to consummate a sale," said Tenenbaum. "With RSA public key cryptography, however, one can authenticate the identity of trading partners so that access to sensitive information can be properly accounted for."

This secure version of NCSA Mosaic allows users to affix digital signatures which cannot be repudiated and time stamps to contracts so that they become legally binding and auditable. In addition, sensitive information such as credit card numbers and bid amounts can be securely exchanged under encryption. Together, these capabilities provide the foundation for a broad range of financial services, including the network equivalents of credit and debit cards, letters of credit and checks. In short, such secure WWW software enables all users to safely transact day-to-day business involving even their most valuable information on the Internet.

According to Joseph Hardin, director of the NCSA group that developed NCSA Mosaic, over 200,000 copies of the interface software are being downloaded monthly from NCSA's public server — well over a million copies to date. Moreover, five companies have signed license agreements with NCSA and announced plans to release commercial products based on NCSA Mosaic.

At the CommerceNet launch, Allan M. Schiffman, chief technical officer of EIT, demonstrated a working prototype of secure NCSA Mosaic, along with a companion product that provides for a secure WWW server. The prototype was implemented using RSA's TIPEM (Toolkit for Interoperable Privacy-Enhanced Messaging) Software Developer's Kit.

Any user that is familiar with NCSA Mosaic should be able to understand and use the software's new security features. Immediately to the left of NCSA's familiar spinning globe icon, a second icon has been inserted that is designed to resemble a piece of yellow paper. When a document is signed, a red seal appears at the bottom of the paper, which the user can click on to see the RSA public key certificates of the signer and issuing agencies. When an arriving document is encrypted, the paper folds into a closed envelope, signifying that its information is hidden from prying eyes. When the user fills out a form containing sensitive information, there is a 'secure send' button that will encrypt it prior to transmission.

Secure-HTTP enables incorporation of a variety of cryptographic standards, includ

Continued on page 5

ORACLE Licenses RSA Security Software

REDWOOD SHORES, March 15, 1994 — Oracle Corp. and RSA Data Security announced today that Oracle has licensed several security techniques from RSA, including the RC4, MD5, and Diffie-Hellman encryption technologies for inclusion in Oracle's SQL*Net networking software. SQL*Net, which is currently available on all major hardware platforms, provides transparent data sharing between Oracle database servers, client applications, and third party data management systems, even across heterogeneous network protocols. Oracle is the first major DBMS vendor to offer network data encryption in response to customer calls for increased security.

Larry Ellison, President of Oracle, called the agreement ''Significant, in that RSA's technology complements the sophisticated security mechanisms found in Oracle7 and Trusted Oracle7 by extending the high degree of data protection across the entire enterprise. Truly distributed applications can now be safely deployed in industry segments like the finance community, which are currently very exposed to data theft or modification during transit. In addition to being the first to offer this technology, the way we are deploying it is also very interesting, since we allow the compute-intensive operations involved in encoding the data to be spread out across all of the processors in an SMP or massively-parallel computer system."

"Anyone not using a secure link between their client applications and database servers is inviting disaster," said Jim Bidzos, President of RSA. "Oracle's endorsement of RSA technology means that this is the birth of a new de facto standard for transmission of secure data between SQL-based applications and SQL database engines."

SQL*Net is Oracle's open networking layer which allows Oracle and third party products to operate transparently over virtually any network protocol, including SPX/IPX (Novell), TCP/IP, SNA, DECnet, Banyan Vines, Named Pipes, NetBIOS, OSI, AppleTalk, X.25, MaxSix, Async connections, and others.

"What we are offering is very unique. Since it is purely a software product it can be installed at very low cost on virtually any existing computer system, instead of having to install expensive hardware encryption boards or black-boxes," said Laurie Mann, Senior Product Manager for SQL*Net, Oracle. "This product not only works with Oracle7, but with a whole host of other database management systems supported by our Transparent Gateways, such as DB2. We've also designed it to work with the Oracle MultiProtocol Interchange, which means that for the first time a single product can provide encryption that operates across network protocols. That means that a Windows application on a Novell network can send data up to the corporate mainframe, which uses LU6.2 as the network transport, perhaps running through a TCP/IP or DECnet network or two on the way up, and the data stream is fully protected start to finish. No one else offers this - at any price."

Although pricing and availability has not yet been announced, Oracle says it plans to price the product aggressively to enable widespread deployment. Developers at Oracle used RSA's BSAFE 2.0 software developer's kit to build security for SQL*Net. Oracle Corp., with headquarters in Redwood Shores, Calif., is a leading supplier of information management software. Oracle develops and markets the Oracle7 family of software products for database management, Cooperative Development Environment (CDE), a complete set of CASE and application development tools for enterprise- wide, client/server computing; multi-protocol networking products; and Oracle Applications, packaged client/server solutions for human resources, accounting and manufacturing. Oracle software runs on personal digital assistants, PCs, workstations, minicomputers, mainframes and massively parallel computers. The company offers its products, along with related consulting, education and support services, in 93 countries around the world.

RSA Licensees and Products

For details about these and other RSA licensed products, call or e-mail us for your free copy of the RSA Security Solutions Catalog.

Alcatel TITN
TWICE CDPD Protocol Software

ANS CO+RE
Interlock Secure IP Network Management

Apple Computer, Inc.
System 7 Pro

AT&T
Models 4100 and 3600 Telephones
AT&T Secure Video Docking Unit
AT&T PersonaLink Services

Bankers Trust Company
Bankers Trust Authentication Services

BLOC Development
F3 Forms Automation System

Cincinnati Microwave, Inc.
MC-DART 100 CDPD Wireless Modems

Cycomm Corp.
Secure Cellular Telephones

Datamedia Corp.
SECUREXchange Email Security Overlay

Delrina
PerFORM PRO, FormFlow

Digital Equipment Corporation
(to be announced)

Enterprise Solutions
ES/Secure for Enterprise Mail/400

Fischer International Systems
WorkFlow.2020, Watch Dog, RSA 3270

Funk Software
WanderLink remote access software

GE Information Services
GEIS Secure NW Services

General Magic, Inc.
Telescript & MagiCap

Global Village Communications
(to be announced)

HILGRAEVE HYPERACCESS/5
Secure Remote Access

HUGHES
NetLock Secure TCP/IP

IBM
4755 Adapter, 4753 Network Security Processor

LOTUS DEVELOPMENT CORP.
Lotus Notes

MICROSOFT CORP.
Windows for Workgroups, At Work, Cairo (coming soon)

MOTOROLA, INC.
Commercial Secure Telephone Units

NATIONAL SEMICONDUCTOR CORP.
iPower PCMCIA crypto cards

NEWBRIDGE NETWORKS
TAP System Network Encryption Devices

NORTHERN TELECOM
X.25 Packet Data Security Overlay

NOVELL, INC.
Netware 3.11 and 4.0

ORACLE CORP.
SQL*Net

PCSI
Ubiquity* 1000 CDPD Mobile Communications Module

RACAL DATACOM
Datacryptor Link Encryption Devices

RETIX
ROUTERXchange* RX 7000 MD-IS CDPD Router

SCI/ICTI
Ruggedized secure military telephones

SEMAPHORE COMMUNICATIONS CORP.
Ethernet & Token Ring Network Encryption Units

SUNSOFT
Solaris Secure NFS and Secure RPC

TRUSTED INFORMATION SYSTEMS
T-Mail and TIS/PEM

UNISYS CORP.
(To Be Announced)

WORDPERFECT CORP.
InForms

General Magic Picks RSA for Telescript™ and Magic Cap™

Earlier this year, General Magic announced that it had licensed technology from RSA Data Security, Inc. to provide security services for its new Telescript™ communications engine. Telescript is a powerful language developed by General Magic to promote the widespread use of secure, intelligent electronic agents. General Magic's developers used RSA's BSAFE™ Cryptography Toolkit to provide Telescript with advanced encryption and digital signature features based on the patented RSA Public Key Cryptosystem™ and RSA's RC4™ symmetric stream cipher, the fastest encryption scheme commercially available. RSA's technology will be crucial to ensuring the security of data on the General Magic's Magicap™ platform and traveling over AT&T's PersonaLink™ Services, a new communications network based on Telescript.

General Magic's Personal Intelligent Communicators are designed to help people organize their lives, learn more effectively, communicate with other people, play and have fun, and know more about their world. The communicators are designed to be simple to use and will come in a range of models to fit many budgets, needs and tastes.

RSA President Jim Bidzos said, "Most wireless communications systems are security nightmares. They have no real encryption, no authentication — a hacker or competitor can easily pull your sensitive data out of thin air. General Magic realized that for a lot of people, wireless services of any kind simply can't be trusted. So they built RSA encryption and authentication services right into the foundation of Telescript and Magic Cap. By taking responsibility for addressing the security problems inherent in wireless technologies, General Magic has given Telescript developers and end users one less thing to worry about."

"The Telescript communications language is an excellent place for powerful security capabilities. By building in RSA security technology at the 'ground floor', and providing a simple interface, General Magic has made it possible for 3rd party application developers to seamlessly integrate secure, interoperable privacy and authentication features into their products. The winner is the user of those products."

Telescript is to networking what PostScript™ is to printing. It is a powerful object-oriented programming language developed by General Magic to promote the widespread use of secure, intelligent electronic agents. Communicating applications built with Telescript will go beyond traditional electronic mail to provide systems supporting electronic commerce, transaction services and electronic data interchange.

General Magic was formed in May, 1990, as a spinoff of Apple Computer with strategic partners including AT&T, Motorola, Sony and Phillips.

NCSA Mosaic *continued from page 3*

ing PKCS #7 and Internet Privacy Enhanced Mail (PEM). CommerceNet will certify RSA public keys on behalf of member companies, and will also authorize third parties such as banks, public agencies, industry consortia to issue keys. Such keys will often serve as credentials, for example, identifying someone as a customer of a bank, with a guaranteed credit line. Significantly, all of the transactions involved in doing routine purchases from a catalog can be accomplished without requiring buyers to obtain public keys. Using only the server's public key, the buyer can authenticate the identity of the seller, and transmit credit card information securely by encrypting it under the seller's public key.

Information on Secure NCSA Mosaic can be obtained by sending e-mail to shttp-info@eit.com.

RSA Labs Update

The increased Labs activity of 1993 has continued without break into 1994 and, in what we expect to be an exciting year for RSA Laboratories, we will be widening our horizons even further. Technical support and independent consulting continue, but an emphasis on current cryptographic research has been a pleasing by-product of our continual review of the current literature. We expect this trend to continue with the addition of a new research scientist in the summer and the consequent broadening of our cryptographic expertise. We are now in the position to offer additional technical reports which survey the current state of the art in block and stream ciphers, as well as the keenly awaited results of a comprehensive analysis of RSA's very popular stream cipher, RC4. This report will be available under conditions of non-disclosure, as will a companion report on RC2 which we expect to become available in the summer.

As well as providing a day of technical sessions at the successful RSA Data Security Conference in January we also presented a motivational proposal for a block cipher based on MD5 at the Fast Encryption Workshop in Cambridge, UK. and published the first draft of PKCS #11. This new addition to the family of Public-Key Cryptography Standards contains details on a standard cryptographic interface for smart tokens and comes at a particularly timely stage in their development and increasingly widespread use.

1994 RSA LABORATORIES SEMINAR SERIES

The RSA Laboratories Seminar Series is now becoming a tradition — the third week of August is the time to come to California and learn about cryptography! The first series laid the foundations with detailed cryptography seminars ranging in material from the most recent theoretical results through to practical issues in the implementation of RSA. The emphasis in the first series was on providing a good basic all-around education in cryptography. This emphasis remains unchanged for the second series, but we will be providing a parallel track for those already well-versed in crypto basics. We anticipate the addition of many new topics; we will be including sessions on secret-sharing, RC2, RC4, authentication protocols, DES, elliptic curves, zero-knowledge schemes and RSA hardware.

The seminars, which should be happening about the time you receive this newsletter, will suit those traveling to Crypto'94 (which takes place the following week in Santa Barbara) as well as those who just want to get up to date with what's happening in cryptography.

The Arcade Project: A Progress Report

CD-ROMs are being increasingly used for the distribution of large amounts of data, and many vendors wish to ensure that retrieval of data from the disc can only take place after the necessary approval has been given; for instance, after payment of fees. The data on the disc can be encrypted using conventional cryptographic techniques... but since all the discs in a production run are identical, how do you prevent a malicious user from passing on the unlocking information? Solving this dilemma is the goal of the ARKD (Abuse-Resistant Key Distribution) Project, aka "Arcade".

Current solutions generally require that some unique secret information, perhaps a DES key, is stored in a tamper-proof environment which forms part of the disc-reading system. This key is used to encrypt the unlocking information that is sent, perhaps via telephone, to the user. Each user's decrypting unit contains a copy of the relevant key, and so the information received can be decrypted and used to unlock the CD-ROM. The only information a user sees (and could redistribute) is the encrypted unlocking information, which is only relevant to his decrypting unit.

While cryptographically this solution works well it has two drawbacks. First, each decrypting unit must contain unique identifying information. Second, this information must be kept hidden from the user. Unfortunately, much of the advantage gained by using CD-ROMs is then lost due to the administrative requirements that come with distribution of thousands of unique tamper-proof readers.

We will describe a system as "abuse-resistant" when the task of helping another user to gain unauthorized access to a CD-ROM file is either 1.) traceable to those cheating or 2.) requires as much effort as passing on the entire file.

Arcade is a software-based abuse-resistant object distribution system. It relies on cryptographic techniques to ensure that any unauthorized access to part of the disc requires as much effort as directly re-distributing the recovered information. With previous solutions, the communications between the user and the CD-ROM distributor take place via two channels: the CD-ROM itself and the telephone. Arcade adds a third channel. This allows unlocking information to be split into two independent quantities: one (the access number) is as large as the objects and is sent using the new channel—while the other (the decryption key) is small and convenient to communicate by telephone.

Each access number is unique and while the number itself is large, it can be identified using a short index number *i*. Similarly, each data object on the CD-ROM can be identified with a catalog or index number *j*. To recover an object M_j a user chooses an access number A_i and then gives the distribution center the indices *i* and j. The center checks that the access number A_i has not previously been used and then computes a short decryption key K_{ij} which is returned to the user by telephone.

continued on page 7

RC4 Report

RSA Laboratories has just completed a thorough and wide-ranging report into the security of RC4. Designed in 1987 by Ron Rivest for RSA Data Security, Inc., RC4 is a fast stream cipher. As well as being considered secure by the designer and reviewers within RSA-DSI, RC4 has been widely licensed and subject to the scrutiny of many independent cryptographers who have examined this confidential and proprietary cipher under conditions of non-disclosure.

The recent review provides, in a single document, the results of a full and, at times, complex analysis of RC4. Though the details of this report can only be divulged under conditions of non-disclosure, the results and conclusions can be described here for the first time.

We found no reason to question the security of RC4 analytically; we felt that a cryptanalyst would have a particularly difficult task in trying to compromise RC4 by more subtle means than exhaustive key-search. We also found that sequences generated using RC4 had a 'good appearance' when analyzed using a wide range of popular statistical tests. In short, we found RC4 to be as secure as we had thought.

For those interested in more details and a full justification of our conclusions, the report will become available under conditions of non-disclosure within the following weeks.

PKCS #11: Cryptographic Token API Standard

By Burt Kaliski

(Revised from a portion of my paper "Standards for Implementation — Public-Key Cryptography in Smart Cards," presented at CardTech/SecurTech '94 (Arlington, VA, April 10-13, 1994).)

Imagine having your cryptographic keys on a small, smart, tamper-proof token you can take with you everywhere. You could secure your communications on any computer system, anywhere, with your own keys. The token could be from any manufacturer; and it could work with any software application. To make this happen requires standards.

Many aspects of such tokens have already been standardized, such as physical characteristics and command sets (see ISO 7816). The Personal Computer Memory Card International Association (PC/MCIA) has published a set of specifications for smart memory cards. There are also a number of proprietary token architectures.

What remains to be standardized are two things: specific cryptographic commands for each underlying technology, and a high-level software interface independent of that technology.

RSA Laboratories recently joined with a number of software and hardware manufacturers to develop the software implementation. Called Cryptoki (short for "cryptographic token interface"), the software interface is currently being reviewed and implemented. When finalized, it will become part of PKCS #11, the eleventh member of the Public-Key Cryptography Standards series developed by RSA Laboratories and representatives of the computer industry.

In Cryptoki, tokens consist of two logical areas: an object system and a functional unit. The object system stores data. The system is hierarchical; each object may have any number of child objects. The functional unit performs cryptographic and other functions, both on internal data stored in registers, and on external data. This logical view of a token is expressed as a set of about 40 software interface routines.

So that all tokens look alike to a software application, a Cryptoki token "driver," provided by the token's manufacturer, translates this logical view of a token to the token hardware, enhancing the hardware with software support if necessary. One example of the split is that some cryptographic functions may be in hardware (e.g., RSA), with others in software (e.g., DES), but from the application's point of view both are handled by the driver. As another example, if the token does not have its own local access control (e.g., keypad or thumbprint reader), the token driver can prompt the user to enter passwords for the token through the host computer.

A "bake-off" where developers can integrate their Cryptoki applications and drivers is being planned, and a PKCS #11 standard is expected shortly thereafter. The PKCS #11 development process is still open for additional participants. For more information, call RSA Laboratories, or send electronic mail to pkcs–11–dev–request@rsa.com.

Arcade *continued from page 6*

This decryption key can only be used with the relevant access number to unlock the chosen object. Provided each access number is used only once, there appears to be no efficient way to compute another valid access number or decryption key which would allow access to a different object on the disc. Moreover, since the access numbers are unique and the relation between them difficult to infer, the decryption key (which is short) is useless to any other user unless the access number is passed along with the decryption key. Since the access number is as large as the object this requires as much effort as simply passing on the unlocked object.

An access number is only identified with an object at the time of decryption; consequently, the distribution of access numbers is particularly easy since they could be sold through retail outlets or distributed widely using conventional mail.

RSA-129 Finally Factored

Computational effort expended falls within range predicted by RSA mathematicians.

Arjen Lenstra and his team at Bellcore are to be congratulated for their factorization of the number known as "RSA-129", a "challenge number" first published in the August 1977 issue of Scientific American, in a column by Martin Gardner on the "RSA Public-Key Cryptosystem"

The 129-digit challenge number was:

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

whose two prime factors were found as the result of this factoring effort.

The RSA public-key cryptosystem depends on the difficulty of factoring such numbers (which are the product of two large prime numbers) for its security. Fortunately, prime numbers come in all sizes. (Prime numbers are numbers that are divisible only by themselves and one, such as 2, 3, 5, 7, 11, 13, ...) Thus the user of an RSA public-key cryptosystem can choose prime numbers sufficiently large to defeat even the most determined attacker.

In our 1978 RSA article we recommended using two prime numbers of 100 digits in length (yielding a 200 digit product to be factored); this recommendation still seems quite sound, since factoring a 200-digit number is much much harder than factoring a 129-digit number. And, of course, using numbers that are even larger is quite straightforward.

The new accomplishment does not "break" the RSA Public-Key Cryptosystem. That is, it does not provide a general method for defeating the RSA cryptosystem. Rather, it provides a very useful "benchmark" on the difficulty of factoring numbers, and thus provides very useful guidance to users of the RSA cryptosystem as to how large their prime numbers should be.

Indeed, the factoring of RSA-129 helps to calibrate and confirm previously derived formulas estimating the amount of work required to factor numbers of various sizes. The actual amount of work required to factor RSA-129 was within a factor of four of the amount of work predicted for this task by the estimation formula in the original 1978 "RSA paper" — a very good estimate, cryptographically speaking, where estimates are typically ranged in orders of magnitude. The experience gained in this factoring accomplishment will help improve estimates of the amount of work required to factor even larger numbers.

As part of its effort to calibrate the difficulty of factoring, RSA runs an ongoing contest (with cash prizes) for factoring RSA numbers of various sizes. The RSA-129 number is the fourth such number to be factored. Numbers which have been successfully factored so far include RSA-100, RSA-110, and RSA-120, of lengths 100, 110, and 120 digits each. The next number, RSA-130, and the remaining numbers (RSA-140, RSA-150, ..., RSA-500), are presently unfactored. Roughly speaking, each increase of 10 digits in the length of the RSA number increases the difficulty of factoring by roughly another factor of 5 or 6.

More information on the RSA Factoring Challenge can be found by sending internet email to "challenge@rsa.com", or by calling RSA Data Security at 415-595-8782.

Smallest 5 unfactored numbers in Challenge:
RSA-130 (130 digits)
RSA-140 (140 digits)
RSA-150 (150 digits)
RSA-160 (160 digits)
RSA-170 (170 digits)

Size of award kitty on 4/1/94 will be: $7,923

[It is interesting to note that factoring RSA-129 will earn the factorers a prize of $100, whereas if they had factored RSA-130 instead (which is only one digit longer) they would earn a prize of almost $8000. In any case, the prize money is minuscule compared to the cost of the computing resources required for these efforts...]

Once again, it should be emphasized how important this sort of work is to the practical utilization of cryptography. For example, it is well known that NSA has both "codemakers" and "codebreakers," and that assessing the strength of a code requires vigorous efforts at breaking it. It is

continued on pg. 9

Bruce Heiman on Domestic and Overseas Encryption

Cont'd from page 2

or it doesn't.' And then they say 'Well maybe ... well, you know, maybe there are back doors in *all* these programs. Maybe there is a plain text spit-out. Maybe all the governments have colluded so that really it is not a problem.'

Well, maybe — but I don't think so....when we lobbied this issue in 1992, 1991 (Fall 1991) it was very difficult to lobby when they actually throw everybody out of the room (even up in Congress) and they debate the Amendment in closed-door session. ...I don't know what they said but the House passed the provision. It was partially as a result of that that an accommodation was reached in 1992 permitting exports of RC2 and RC4 (only if used with 40-bit keys) for encryption; prior to that (the permitted keysizes) had been significantly less than that. Certainly right now industry, I think, strongly feels that as a minimum they need to be able to export programs and products employing DES or RC2 or RC4 at comparable key lengths (56 bits or better) ....

The bill number is HR 3627; now I will do my pitch: 'All of you have elected representatives. Contact them, tell them you are interested, get them to co-sponsor this legislation.' It has to be taken out from the bureaucracy, it is a political matter, it is appropriately a political matter - and we all will be trying to show support.

Thank you. (Audience Applause).

1994 RSA Data Security Conference

Continued from page 1

products. General Magic announced that it will use RSA encryption and authentication in its Telescript language and Magic Cap environment. Hewlett-Packard announced the availability of a cryptographic security module for its HP 9000 UNIX-based business server. National Semiconductor unveiled a new hardware technology called iPower. It's a tamper-resistant RSA-encrypting PCMCIA smart card that includes a microprocessor, non-volatile memory, and associated hardware.

Other electronic mail security products were well represented. Steve Kent of BBN Communications and Steve Crocker of Trusted Information Systems discussed Privacy Enhanced Mail (PEM) products and services. Enterprise Solutions showed their secure X.400 equipment, and Datamedia Corporation showed their SECUREXchange product.

A new company, Digital Timestamping, Inc., announced a new system for commercial implementations of secure digital timestamping of digital documents. The idea is to be able to prove that a digital document existed at a certain date, without having to store a copy of the document with a trusted authority. The protocols behind this scheme are discussed in my book as well.

Martin Hellman of Stanford University discussed recent attacks against DES. He also presented a new result: an attack against eight-round DES that combines techniques from linear and differential cryptanalysis. The attack is much faster than any previously known attack, but at this time cannot be extended to full sixteen-round DES. Ron Rivest of MIT discussed advances in factoring large numbers (important for the security of RSA), and Cetin Koc of Oregon State University discussed high-speed software implementations of RSA.

In only three years this conference turned from a small meeting of RSA licensees to a major industry gathering. We hope you'll join us next year!

Public Key Cryptography is Not Easy to Break

Bill Payne sent me a copy of his draft paper "Public Key Cryptography is Easy to Break" and gave me permission by phone to post a description.

The quick summary is that his result, while clever, actually confirms that RSA is still hard to break.

RSA BACKGROUND

An RSA key pair consists of a public key (n, e) and a private key (n, d), where n, the RSA modulus, is the product of distinct primes p and q, and where e and d (respectively the public and private exponents) satisfy the equation

$$e\,d = 1 \bmod (p-1)(q-1)$$

To break RSA (i.e., solve for the private key, given the public key), one need only find the product $(p-1)(q-1)$, which is usually denoted $\phi(n)$. Given $\phi(n)$ one can easily find p and q, so a method that finds $\phi(n)$ also factors n.

PAYNE'S RESULT

According to Fermat's little theorem, for all a, one has

$$a^{\phi(n)} = 1 \bmod n$$

Consequently, for $a = 2$, one has that $2^{\phi(n)}-1$ is divisible by n. One can therefore find $\phi(n)$ (or a divisor of it) by constructing a multiple of n whose binary representation is all 1's.

Payne's algorithm finds such a multiple by simple binary operations. The algorithm sets bits of an accumulator to 1 by adding shifts of the modulus n, working from least significant to most significant bit of the accumulator. Eventually the accumulator is all 1's, and the number of 1's yields a divisor of $\phi(n)$.

Here is the algorithm:

```
x := 0
i := 0
while x contains a 0 bit
(other than leading bits) do
    if bit i of x is 0
        then x := x + (n·2^i)
    i := i + 1
return length of x in bits
```

By considering only the window of bits starting at bit i, one can view Payne's algorithm as applying repeatedly the following permutation on the set $\{0, ..., n-1\}$:

$$f(w) = \begin{cases} (w + n - 1) \,/\, 2 & \text{if } w \text{ is even} \\ (w - 1) \,/\, 2 & \text{if } w \text{ is odd} \end{cases}$$

The window w at iteration i corresponds to the accumulator value $x = 2^i w + 2^i - 1$. Since the function f is a permutation, repeated application of f will eventually return to any given starting value. To find a multiple of n whose binary representation is all 1's, it suffices to start with $w = 0$. When repeated application of f arrives at $w = 0$ again, the value $x = 2^i - 1$ will be a multiple of n whose binary representation is all 1's.

There's only one problem: Finding x can take up to $\phi(n)$ steps! Since $\phi(n)$ is almost as large as n, if n is just tens of digits long (not to mention the hundreds of digits in RSA), the amount of work is enormous. Indeed, this is an "exponential-time" algorithm for finding $\phi(n)$, the slowest kind. While Payne's algorithm is curious, public key is no easier to break.

— Burton S. Kaliski, Jr.

RSA-129 Factored

Continued from page 8

widely believed that the Germans might have had greater success in World War II if their codebreaking and codemaking efforts had been better integrated. The efforts of Mr. Lenstra and his Bellcore team are precisely the kind of work needed to assess the strength of the RSA cryptosystem and to guide users of the RSA cryptosystem in choosing the lengths of their RSA keys.

— Ronald L. Rivest

Triple-DES

Three recent results have confirmed the predictions many made in the late 1970's that the Data Encryption Standard would by now be nearing the end of its useful lifetime:

- Eli Biham and Adi Shamir's differential cryptanalysis of the full 16-round DES, presented at CRYPTO '92, which breaks DES with 2^{47} chosen plaintexts. It is the first attack requiring less work than exhaustive search through the 2^{56} possible keys.
- Mitsaru Matsui's linear cryptanalysis of DES, presented at EUROCRYPT '93 and recently improved, which has already broken DES experimentally with 2^{43} known plaintexts (this took 50 days on 12 HP 9740 workstations).
- Michael Wiener's design for a $1,000,000 exhaustive search engine, described at CRYPTO '93, which can find a DES key in 3.5 hours.

For many applications DES is still adequate, especially if the keys are changed often. But for critical data, and in the long term, what is the alternative? No secret-key cryptosystem has received the attention that DES has. Some are adopting new algorithms such as RSA Data Security's RC2 block cipher and RC4 stream cipher, and the IDEA algorithm developed by Xeujia Lai and James Massey, all of which offer potentially better security than DES. Others are considering triple-DES, with three DES operations per block.

Triple-DES has been around for a long time as a method of encrypting keys. The ANSI X9.17 standard, for instance, defines the so-called "EDE" mode of DES involving two DES keys, which encrypts with the first DES key, decrypts with the second, and encrypts with the first again. A variant of this mode, generally considered stronger, involves three different DES keys. Brute-force attacks on triple-DES take at least 2^{112} operations, compared to just 2^{56} for ordinary DES.

For multiple-block messages, there are many options, depending on how one interconnects the three DES operations. Two of recent interest are "inner-CBC" and "outer-CBC", both generalizations of ordinary cipher block chaining (CBC) mode, which exclusive-ors a plaintext block with the previous ciphertext block before encrypting. In inner-CBC mode, this "feedback" happens three times, once for each of the three DES operations. In outer-CBC mode, it happens only once, around all three.

Security and performance of the modes are quite different:

- Inner-CBC is potentially faster. Since the feedback is around each DES operation, one can achieve the same speeds as ordinary DES, given three DES chips. In outer-CBC mode, even with three chips, the performance on a single message stream is at best one third that of ordinary DES, because of the long feedback.
- Inner-CBC also appears more secure against exhaustive search, because the internal feedback values are unknown to an attacker. In essence, they act as additional secrets.
- Outer-CBC is much better against differential cryptanalysis involving chosen ciphertext. Eli Biham has shown that inner-CBC is essentially no more secure against this kind of attack than ordinary DES is. The main reason is that by choosing ciphertext, an attacker can control the internal feedback, and thereby break the three DES operations one at a time. While this kind of attack is not very practical, it does demonstrate a "certificational weakness" in inner-CBC.

Based on these observations, RSA Laboratories is recommending outer-CBC mode for triple-DES. The specific mode suggested is called "DES-EDE3-CBC": three DES keys, the first and third for encryption and the second for decryption, with cipher block chaining on the outside. A full RSA Laboratories report on triple-DES and its modes is in preparation.

— Burton S. Kaliski, Jr.

Recent & Upcoming RSA Trade Show Appearances

ELECTRONIC MESSAGING ASSOCIATION '94
Anaheim
April 18 – 21

NETWORLD/INTEROP '94
Las Vegas
MAY 4 – 6

GROUPWARE '94
San Jose
AUG 9 – 11

NETWORLD/INTEROP '94
Atlanta
SEP 12 – 14

NATIONAL COMPUTER SECURITY EXPO (CSI) '94
Boston
NOV 13 – 15

ter to her in late July derailed that effort in favor of the series of "studies" mentioned earlier, which will also evaluate the impact of export restrictions on U.S. competitiveness in the international marketplace.

Embarrassing Design Flaws

On June 1, the New York Times broke the story of a basic design flaw in the algorithm used in Clipper. Dr. Matthew Blaze had been testing the government's "Tessera" PCMCIA card, and managed to spoof the Law Enforcement Access Field (LEAF), subverting the enforced key-escrow characteristics of Clipper and making a spoofed chip useless for law enforcement. (Tessera, like Clipper, uses the Skipjack algorithm.) This design flaw, coupled with the design flaw discovered several months ago in the Digital Signature Standard's hash algorithm, have proved extremely embarrassing (and expensive) for the government, requiring the recall of tens of thousands of already-issued Tessera cards. Clearly, the government will have to provide some type of "fix" for these flaws before these methods can be widely implemented, even inside the government.

Patent troubles for DSS

Announced on February 4 by NIST as a "royalty-free digital signature standard," and published as FIPS 186 on May 19, the government has yet to obtain the necessary patent licenses for the technology from Public Key Partners, the patent-management company established by the inventors of public key cryptography. While NIST claims that DSS infringes no patents from PKP, they have been privately negotiating with PKP for over a year. PKP has already threatened to sue any private company that implements DSS without a license.

While DSS is mandated for use in US Federal government agencies "and companies doing business with them" effective December 1, 1994, NIST has been advising private companies to wait for the legal wrangles to be over before introducing DSS-based products.

DSS: Reinventing the Wheel?

Meanwhile, even government agencies are complaining about the imposed necessity to support two incompatible signature schemes, when the RSA infrastructure is already well established. NIST announced in June that "in about a month" it would issue cryptographic application program interfaces (APIs), despite the existence for over three years of PKCS, the industry-created open API for public key crypto. Over six million copies of RSA-based cryptography and/or digital signature software are already installed in the marketplace. The Internal Revenue already uses RSA-based crypto with banks, and IRS management has repeatedly stated that it will be difficult to convince the commercial banking industry to change or to maintain dual systems. IRS is also concerned about the lack of a government-operated certification authority to issue DSS-based certificates and validate them on request - an infrastructure that already exists in the RSA-based commercial arena.

— Dana C. Ellingen

CipherText Survey

Be one of the first 100 people to complete & fax back this survey, and you'll win a free SINK CLIPPER T-shirt! Fax RSA at 415-595-1873.

Name _____

Title _____

Company _____

Address _____

City, State, ZIP _____

Phone _____

E-Mail _____

☐ Check here if this is a new address for you

☐ Check here if you would like an RSA representative to contact you.

How do you rate this edition of CipherText?

Personal Interest Level:
Very Interesting 1 2 3 4 5 Not Interesting

Informativeness:
Very Informative 1 2 3 4 5 Not Informative

Technical Level:
Too Technical 1 2 3 4 5 Too Simplistic

Overall:
Great Stuff 1 2 3 4 5 Junk Mail

Please suggest a topic for a future article:

_____

_____

Please suggest a future guest columnist:

_____

_____

Please suggest a product category for a future product spotlight:

_____

_____

How would you describe your interest in RSA technology?
☐ Academic
☐ Looking for a finished product with RSA inside
☐ Developing a product for my company's use
☐ Developing a product for my company to sell
☐ Already an RSA licensee

If you can, please briefly describe any project you might be working on that has a need for crypto/security:

_____

_____

_____

_____

Is your company considering licensing any RSA toolkits or technologies? YES NO

If yes, how soon?
Within... 30 days 90 days 180 days 1 year

Thank you!

RSA Announces Free Software for Personal or Corporate Use

This past March RSA announced new versions of RIPEM and RIPEM/SIG: encryption/signature and signature-only "freeware" that implements RSA's patented encryption and digital signature technologies.

The announcement is significant because it is the first time ever RSA's popular, patented encryption and authentication technology has been made available at no charge whatsoever for use in commercial settings. RSA has already applied for and received a Commerce Department "Commodities Jurisdiction" from the U.S. State Department for RIPEM/SIG, which allows that software to be freely exported.

Information superhighway gets free tool to encrypt & authenticate information; an answer to Vice-President Gore's concerns over Internet break-ins.

RIPEM and RIPEM/SIG are built on top of RSA's popular freeware RSAREF (pronounced "R.S.A. reff" short for "RSA reference implementation") cryptography toolkit — but until now, RSAREF was only approved for individual usage. Now RSA has relaxed the use restrictions for RSAREF, and any application built with it may now be used by individuals or companies so long as it (or services based on it) are not sold. In other words, RSAREF and RIPEM are free so long as they are free to everyone "on down the line".

The RIPEM application was developed by Mark Riordan of Michigan State University, using RSA's RSAREF toolkit . A Macintosh version, developed by Ray Lau of MIT, the author of the popular "Stuffit" program, is also available. Versions for DOS, Mac, Unix, and all popular platforms are supported. The "PEM" in RIPEM stands for Privacy Enhanced Mail, a published Internet standard for secure electronic mail.

To download RSAREF, RIPEM or RIPEM/SIG, send any e-mail message to rsaref@rsa.com or anonymous ftp to ripem@ripem.msu.edu.

RSA DATA SECURITY, INC.
100 MARINE PARKWAY
SUITE 500
REDWOOD CITY
CA 94065-1031

FIRST CLASS MAIL
ZIP + 4 PRESORT
U.S. POSTAGE PAID
MMS, INC.