Encryption and Networking Applications

John Long

The DOE requires that sensitive unclassified data be protected while being transmitted electronically. On most large networks it is difficult and expensive to provide the required level of physical protection. At Sandia National Laboratories, we are assembling the structure necessary to protect sensitive unclassified data using software-based encryption. This approach has the advantage that the data can be protected after arrival at its destination without additional investment. While Sandia has expertise in cryptography, we had not used cryptography in this field. This discussion deals with the client-server model of file-based data exchange and interactive access to on-line data bases using Unix workstations, Macs and PCs.

DOE Requirements

At the outset, we knew that DOE requires the use of DES (the Data Encryption Standard) when encryption is used to protect unclassified data. It was impractical for us to implement widespread use of DES with manual key distribution because of the potentially large numbers of DES keys. We found two possible techniques that seemed to skirt the issue acceptably: Diffie-Hellman key negotiation and public-key distribution of DES keys. Our initial investigations led us to believe that use of public-key encryption would violate DOE and NIST (the National Institute of Science and Technology) policies. However, in subsequent conversations with NIST we learned that using commercial software for public-key distribution of DES keys is allowed by FIPS (the Federal Information Processing Standards) until a FIPS-approved public key-based key distribution technique is established (FIPS PUB 140-1, Sec. 4.8.2, p. 30). In further discussions with DOE, they found this acceptable. This breakthrough opened the door to use of several commercially-available software encryption packages.

In summary, the DOE requires that our software: 1) use DES encryption, and 2) generate electronic signatures meeting the DSS (Digital Signature Standard) specification. The use of SHA, the Secure Hash Algorithm, is required as part of DSS. If single-use DES keys are encrypted separately and transmitted as part of the message (a widely-used technique), they can be encrypted using public key techniques. An additional self-imposed requirement is that the software run on Windows, DOS, NT, Macs, and Unix workstations. Some commercially-available software has been tested which meets these criteria. Note: DSS signatures are not compatible with the well-known digital envelope / digital signature technology from RSA Data Security, Inc.

The Need for Other Encryption Techniques

Meanwhile, a broader view of the situation developed. Our chosen technique for protection of sensitive data, selecting encryption software and obtaining a site license for that package, was also expected to contain the cost of software. A second, very expensive technique for protecting sensitive unclassified data would use secure hubs in our network and eliminate the need for encryption software. But neither technique, while protecting sensitive unclassified data acceptably, addresses the general encryption problem that faces our average staff member. The general problem occurs when we interact with the outside world and receive electronically-

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.

signed E-mail, or if we download from a web server using secure Mosaic, or any number of other situations demanding that we match encryption techniques used on the Internet.

Also, our staff who are involved with CRADAs (Cooperative Research and Development Agreements) use E-mail to communicate extensively with their CRADA partners. In some cases, E-mail replaces telephone communications over long periods, leading to a need for authentication of messages. Large amounts of proprietary data are often involved, and the CRADA partner may already have a significant investment in software for signing and encrypting attachments to electronic mail. It is important that CRADA agreements address the requirements for protection of proprietary data, including encryption.

File Encryption -- A Partial Solution

Additionally, our internal customers who transmit sensitive unclassified data inside Sandia need to interact with their customers in various ways, resulting in the need for multiple types of encryption software. Our organizations that produce reports for managers run their report generators at night when the interactive load is light. This type of use requires software to encrypt the sensitive reports attached to machine-generated electronic mail. Other standard reports, also sensitive and available to groups of managers, must be accessible interactively during normal business hours. This demands an interactive encrypted link such as secure Mosaic.

The Need for Digital Signatures

Finally, the need to interact on the Internet will often require the use of digital signatures and encryption. While not many of our staff have yet reached that point, this sort of usage will increase. For example, important E-mail messages on the Internet are now often signed. While we seldom feel the need to validate these signatures, this will become more desirable as the sophistication of hacker attacks increases and the type of attack varies. A bogus message has already been used to "cancel" a final exam at a major university.

No Single Standard

Given these broader requirements, it was our hope to discover trends on the Internet that would allow us to standardize on the type of protected communication that will eventually be dominant. Unfortunately, the Internet world is still in a phase of development often seen in technical areas, characterized by high levels of innovation and rapid proliferation of new products. At this point, most participants have no desire for format standardization in encrypted messages. To be sure, the government is applying pressure in every way possible to encourage standardization, as are certain commercial firms. But each of these participants has their own agenda, resulting in controversy and lawsuits. To make matters worse, the questions of privacy and wiretapping are central to some of the issues, with export controls of less concern to many participants but no less enmeshed in the controversy.

A majority of people who use personal computers to send secure or signed E-mail on the Internet are using PGP (Pretty Good Privacy), even though PEM (Privacy Enhanced Mail) is a draft Internet standard. On the other hand, PEM is installed on many Unix workstations. Normally, any draft standard would be chosen without question. However, users of personal computers have a numerical advantage on the Internet, and this group has little use for standards.

Instead, they prefer to let demand set the standard. Both products, if used properly, appear to provide good security.

The world of secure interactive WWW (World Wide Web) access -- secure browsers -- is more complicated and considerably more turbulent. Our view of this world continues to change daily, and it is therefore premature to address this topic in detail.

In summary, there are many products in this field -- commercial, freeware and shareware -- and nearly every one is unique and incompatible with all others in some way. But if we wish to receive communications from people using these various packages in the future, we will be forced to obtain the ability to decrypt their messages and/or authenticate the signatures. Thus, those who take advantage of information on the Internet will find increasing need to own various types of encryption technology besides that meeting DOE requirements. This will result in purchases of various encryption packages, independent of our implementation of protection for sensitive unclassified data. The expenditure in this area will eventually be large, in spite of our efforts.

An Approach to Encryption at Sandia

We intend to publicize the DOE requirements and promulgate a policy specifying an encryption package for internal use. This will minimize switching software packages after the customer has become accustomed to the present software. An associated cost-saving measure is to obtain a site license for the chosen software.

In the case of AT&T Secret Agent, the encryption package of choice for batch access, we can also use the purchase of a site license to hasten the porting of this software to various Unix platforms. The developers are concentrating on platforms that have high demand, and the purchase of a site license will give us leverage to cause porting to other platforms in use at Sandia. Some features that we will eventually need are currently being developed. We can attempt to negotiate an advantageous upgrade plan to bring our customers to a common version at very low cost.

Encrypted interactive access is more difficult. Netscape and perhaps other Web browsers are, or will be, capable of meeting DOE encryption requirements, but they currently lack compatibility with Kerberos or DCE (Distributed Computing Environment) software. Also, unlike servers on the open Web, secure servers currently require compatible browsers. The Web consortium and others are now approaching this issue. Kerberos and DCE security features are secondary issues in the commercial market, but are important at Sandia. We have not yet successfully resolved this issue. (Note: This information reflects our current knowledge, but will be obsolete by the time this is printed. It is a snapshot of our view of technology moving at warp speed.)

Summary & Recommendations

The DOE requires that sensitive unclassified data be protected while in transit. Encryption is one acceptable way of protecting the data. The DOE requirements on encryption software are that 1) it use DES encryption, and 2) any electronic signatures meet the DSS specification. Using SHA, the Secure Hash Algorithm, is required as part of DSS. If single-use DES keys are encrypted separately and transmitted as part of the message (a widely-used technique), they can be encrypted using commercial public key techniques.

Selecting a software package to protect sensitive unclassified data and obtaining a site license will not contain the cost of encryption software. Those who take advantage of information on the Internet will find increasing need to own various types of encryption software.

We are recommending the use of AT&T Secret Agent for bulk file encryption, creating E-mail attachments and other purposes. Costs can be minimized and better coverage of various Unix platforms can be provided if a site license for AT&T Secret Agent is procured for batch access. No known secure web browser meets our requirements.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.