On Implementing Security Extensions to the TCP Transport Layer *

Lawrie BROWN†
Department of Computer Science,
UC UNSW, Australian Defence Force Academy,
Canberra ACT 2600 Australia

Abstract

Computer networks and LANs are becoming an increasingly common component of organisational computing infrastructures. With the spread of internetworks able to link LANs together, and the increasing availability of cheap network hardware which can be used to monitor traffic on a network, the need to add additional security to network services is becoming imperative. This paper details the development of security extensions to the TCP transport layer of the TCP/IP protocol suite used by many computer systems. These extensions will provide authentication of the user and encryption of information exchanged over the network link. These extensions are based on the Secure Data Network System (SDNS) protocols, but adapted to meet requirements here. These include providing security services on certain specific connections, without requiring a major installation reconfiguration of large internetworks; and providing security services to mobile and portable stations over packet radio networks.

1 Introduction

Traditionally it has been assumed that computer networks are secure. In the days when networks were the province of large organisations, and computers were managed by operators in secure rooms, this fiction was acceptable most of the time. With the increasing growth of internetworking, which links LANs together and leads to traffic over a wide area, and the ease of obtaining cheap network computers which can be used to monitor all traffic on a network, there is an urgent need to extend network services to incorporate greater security features.

*This research is supported by ATERB grant N003/011 1992/93
†Email: Lawrie.Brown@adfa.oz.au

One of the common network protocol stacks is the DoD TCP/IP suite, implemented on most Unix systems, and on a wide range of other computers. It is the basis for much of the world-wide internet, and is one of the most extensively utilised protocols in the world. Limitations of this suite from a security perspective have been known for some time [1], [2], [3]. Work on security extensions to TCP/IP has been undertaken from several different perspectives. Firstly, security extensions are being defined for specific application utilities in the upper layers of the protocol suite, including for Telnet and FTP. Secondly several security extensions are being developed for use by the lower layers as a general security service.

The author has been involved in a continuing project concerned with the specification of authentication and encryption services to various network utilities, including Telnet – the remote terminal utility, FTP – the file transfer utility, and others. These utilities are part of the TCP/IP internetworking suite. Until recently, authentication by these services was done by sending a username and password over the channel in the clear, and then exchanging all subsequent information, also in the clear. This ran a risk of security breaches on a conventional wire network, that becomes a virtual certainty on a packet network where any station can passively monitor all transmissions without being detected. To date, an extension to the Telnet protocol has been developed which provides authentication using a challenge-response system, and subsequent encryption of the data exchanged [4]. An initial implementation in software was completed by Jan 1991, followed by a revised version in 1992. Following on from this, authentication and encryption extensions to the FTP utility have been defined, and an initial implementation was written [5]. These extensions are being developed in parallel with work by the Telnet Working group of the Internet Engineering Task Force (IETF) in the US, who are also working on security extensions to Telnet. However their extensions are oriented to using the Kerberos authentication system [6], which is a system for providing security on large networks of computers. This however requires a major reconfiguration of the computers in the system to use it. Our extensions are compatible during the negotiation phase, but are oriented to closed user group applications where minimum changes are required, and where kays may be manually distributed along with account information.

Another working group of the IETF, the Common Authentication Technology (CAT) WG is developing a generic security service API, which may be used by many upper-layer applications. This is currently in early draft, but will be a major factor in future security enhancements to network utilities.

Moving down to lower layers of the protocol suite, a number of security extensions have been proposed. The first of these involve extending the IP (network layer) protocol to include labeling of information, for use by multi-level trusted computing environments. An early extension supporting defense standard labeling was provided in RFC 1038. More recently the Commercial Internet Protocol Security Option (CIPSO) WG of the IETF is developing a

Figure 1: SDNS in the OSI and TCP/IP Protocol Stacks

commercial variation of this. This work has been incorporated into a Multilevel secure TCP product by AT&T [7]. The problem with all of these extensions is that they assume the network cannot alter the IP packet format with the security labels. In a wide-area environment, this is not a valid assumption, and hence these extensions do not address the need being discussed in this paper.

What is required are cryptographic extensions to the TCP (transport) and IP (network) layers to provide the desired authentication and privacy requirements. Early discussion of such extensions is given in [2], [3]. The major realisation of these requirements at present, is through the Secure Data Network System (SDNS) protocols, discussed in the next section.

2 Secure Data Network System (SDNS)

The Secure Data Network System (SDNS) is a joint US government and industry project to define protocols for providing secure communications. It is being coordinated by NIST, and they have published the draft specifications in 3 reports [8], [9], and [10]. These protocols have been designed primarily for compatibility with the OSI Reference Model, although a variant has been specified

Figure 2: SDNS Encapsulated Message

for TCP/IP. SDNS includes protocols in the Application, Transport, Network and Link layers of the OSI stack, with variants for the TCP/IP stack (see Fig ??). An overview of the SDNS protocols is given by Nelson and Heimann [11], and of the key management by Lambert [12]. SDNS is also being considered for use in providing security in ISDN [13]. The SDNS protocols include:

KMP is an application layer protocol for negotiating security parameters, and managing keys for all the lower layer services. It is only defined for the OSI reference model, and uses an X.500 directory service for storing the information. Consequently the use of KMP requires that systems have an OSI stack and X.500 directory service installed.

The security protocols SP4 and SP3 are defined to fit between the Transport and Network layers of the OSI stack, with variants for the TCP/IP stack. The variants SP4 and SP3 share the same functionality; it is a matter of implementation as to whether they are placed at the bottom of the transport layer (as SP4), or at the top of the network layer (SP3). If SP3 is used, then the information may be validated by each link in an internetwork, whereas with SP4, it is for end-to-end protection only. The basic services provided by SP4 and SP3 are confidentiality (through encryption), and connectionless integrity (using an Integrity Check Value (ICV)) Either or both may be negotiated, along with the key to be used, by KMP before communications are established. Connection oriented security is obtained via the transport layer functions provided above the security protocol. The SPx protocols encapsulate the higher layer message into a SPx Protocol Data Unit (PDU) with optionally encrypted and checksummed components, as shown in Fig ??. A clear header indicates which session key was used, and the type of processing which has been performed on the PDU. A number of variations on SP3 and SP4 are defined for specific protocol combinations, including variants for use with TCP/IP, as detailed in [8].

Finally some link encryption protocols are being developed for protecting all traffic on a specific data link.

3 Areas Needing a Secure Transport Service

As detailed in the introduction, the author has been associated with the development of security extensions to various network utilities. This was in response to a need to provide security within a closed user group environment, where minimal changes were desired to the existing computer systems. Rather than continuing to define extensions for each separate utility, it seemed sensible to develop an extension to the network service. This would however, involve a greater modification of system software than had been necessary until now.

Another motivation was based on the increasing usage of portable and laptop computers, traditionally on a standalone basis. However the trend generally in computer usage is toward networking of computers to provide access to shared resources and large information sources. Networking technology is well advanced when the equipment is fixed in one location, but portable and mobile connectivity is not as well established. One technique for providing connectivity to a portable or mobile station is the use of a packet radio network. This allows a number of stations to share a common frequency, on a multiple access channel. A considerable amount of work has been done developing packet radio protocols by a number of organisations, as detailed by Shacham and Westcott [14]. Shacham and Westcott have identified a number of issues as still needing resolution. One of these is the issue of network security, which covers the areas of authenticating the users of the network, providing confidentiality, resisting denial of service attacks, and thwarting traffic analysis. Whilst these are problems on traditional wired networks, they are of much greater concern on wireless networks, due to the greater ease of interception and generation of messages. Much work in this field has been done by the radio amateur community, who have developed the AX25 packet protocol, cf Karn et al [15]. They have an interest in computer connectivity, and have recently being using a TCP/IP implementation known as the NOS (Network Operating System) package to investigate issues raised in this environment [16]. The software is freely available, and is actively being developed by a number of people in the Internet community. It is implemented on PCs and Amigas, and an earlier version NET is available for the Macintosh and Unix systems. It supports both wired (Ethernet, SLIP and PPP connections) and wireless (AX25 packet) networks.

4 An SDNS Implementation under NOS

In this project, it was decided to combine the above motivations by implementing a variant of SDNS in the NOS package. This would enable the evaluation of the protocols over both wired and wireless networks. Also the ready availability of the source makes the implementation easier. Since end-to-end security is the real need in the required applications, SP4 will be the variant implemented. A major area of difference though is with the key management protocols KMP. As defined in the SDNS project, this is implemented only on an OSI stack, using X.500 directory services. Neither of these are known for their compactness nor ease of installation. This also implies a need for a master directory service for the target network. This conflicts with the desire for minimal modifications of the target systems. Consequently we are designing our own key management protocol which will use the challenge-response authentication mechanism previous used in our earlier projects. This only requires coordination between parties wishing to establish secure connections between themselves. The final design of the protocol, and the initial implementation are currently under way. In the future, the extensions may well be ported to other TCP/IP implementations, such as 4.3 BSD.

5 Conclusion

A need has been identified to improve the security of network services. Whilst a number of security modifications have been proposed, none has totally satisfied all local needs. Consequently a version of the Secure Data Network System (SDNS) is being implemented with a modified key management protocol under the NOS TCP/IP implementation. This will provide security services for both wired and wireless networks, with a minimum of changes needed on the target systems.

6 References

[1] V. L. Voydock and S. T. Kent, "Security Mechanisms in High-Level Network Protocols," *ACM Computing Surveys*, 15, no. 2, pp. , June 1983.

[2] W. Diffie, "Security for the DoD Transmission Control Protocol," in *Advances in Cryptology - Crypto 85* (Lecture Notes in Computer Science), vol. 218, H. C. Williams, Ed. Berlin: Springer Verlag, pp. , 1986.

[3] R. Ramaswamy, "Security Architecture for Data Transfer through TCP/IP Protocols," *Computers and Security*, 8, no. 8, pp. , 1989.

[4] L. Brown, "Secure Remote Login - the SECLOG option," in *AUUG 90 Conference Proceedings*. Sydney, NSW, Australia: Australian UNIX Systems Users Group, pp. , Sept. 1990.

[5] L. Brown and M. G. II. Jaatun, "Secure File Transfer Over TCP/IP," in *Proc. IEEE Tencon-92*, Melbourne, Australia, Nov. 1992, Also available as Dept. of Computer Science, UC UNSW, Australian Defence Force Academy TR CS2/92.

[6] J. G. Steiner, C. Neuman and J. I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," in *Proc. Usenix Winter Conf.*. USENIX Assoc., pp. , 1988.

[7] D. A. Futcher, R. L. Sharp and B. K. Yasaki, "Building a Multi-level Secure TCP/IP," AT&T, TR, 1990.

[8] C. Dinkel, "Secure Data Network System (SDNS) Network, Transport and Message Security Protocols," NIST, NISTIR-90/4250, Mar. 1990, Gov't ordering no. NTIS PB90-198946/XAB.

[9] C. Dinkel, "Secure Data Network System (SDNS) Key Management Documents," NIST, NISTIR-90/4262, Mar. 1990, Gov't ordering no. NTIS PB90-188079/XAB.

[10] C. Dinkel, "Secure Data Network System (SDNS) Access Control Documents," NIST, NISTIR-90/4259, Mar. 1990, Gov't ordering no. NTIS PB90-188061/XAB.

[11] R. Nelson and J. Heimann, "SDNS Architecture and End-to-End Encryption," in *Advances in Cryptology - CRYPTO'89* (Lecture Notes in Computer Science), vol. 435, G. Brassard, Ed. Berlin: Springer Verlag, pp. , 1990.

[12] P. A. Lambert, "Architecture Model of the SDNS Key Management Protocol," in *Proc. 11th National Computer Security Conference*, Oct. 1988.

[13] W. E. Burr, "Security in ISDN," NIST, NIST Spec Pub 500-189, 1992.

[14] N. Shacham and J. Westcott, "Future Directions in Packet Radio Architectures and Protocols," *Proc. IEEE*, 75, no. 1, pp. , Jan. 1987.

[15] P. R. Karn, H. E. Price and R. J. Diersing, "Packet Radio in the Amateur Service," *IEEE Journel of Selected Areas in Communications*, SAC-3, no. 3, pp. , May 1985.

[16] P. Karn, NET Users Reference Manual (NOS Version), Mar. 1991.