Network Working Group
Request for Comments: 1704
Category: Informational

N. Haller
Bell Communications Research
R. Atkinson
Naval Research Laboratory

October 1994

On Internet Authentication

Status of this Memo

This document provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

1. INTRODUCTION

The authentication requirements of computing systems and network protocols vary greatly with their intended use, accessibility, and their network connectivity. This document describes a spectrum of authentication technologies and provides suggestions to protocol developers on what kinds of authentication might be suitable for some kinds of protocols and applications used in the Internet. It is hoped that this document will provide useful information to interested members of the Internet community.

Passwords, which are vulnerable to passive attack, are not strong enough to be appropriate in the current Internet [CERT94]. Further, there is ample evidence that both passive and active attacks are not uncommon in the current Internet [Bellovin89, Bellovin92, Bellovin93, CB94, Stoll90]. The authors of this paper believe that many protocols used in the Internet should have stronger authentication mechanisms so that they are at least protected from passive attacks. Support for authentication mechanisms secure against active attack is clearly desirable in internetworking protocols.

There are a number of dimensions to the internetwork authentication problem and, in the interest of brevity and readability, this document only describes some of them. However, factors that a protocol designer should consider include whether authentication is between machines or between a human and a machine, whether the authentication is local only or distributed across a network, strength of the authentication mechanism, and how keys are managed.

2. DEFINITION OF TERMS

This section briefly defines some of the terms used in this paper to aid the reader in understanding these suggestions. Other references on this subject might be using slightly different terms and definitions because the security community has not reached full consensus on all definitions. The definitions provided here are specifically focused on the matters discussed in this particular document.

Active Attack: An attempt to improperly modify data, gain authentication, or gain authorization by inserting false packets into the data stream or by modifying packets transiting the data stream. (See passive attacks and replay attacks.)

Asymmetric Cryptography: An encryption system that uses different keys, for encryption and decryption. The two keys have an intrinsic mathematical relationship to each other. Also called Public˜Key˜Cryptography. (See Symmetric Cryptography)

Authentication: The verification of the identity of the source of information.

Authorization: The granting of access rights based on an authenticated identity.

Confidentiality: The protection of information so that someone not authorized to access the information cannot read the information even though the unauthorized person might see the information's container (e.g., computer file or network packet).

Encryption: A mechanism often used to provide confidentiality.

Integrity: The protection of information from unauthorized modification.

Key Certificate: A data structure consisting of a public key, the identity of the person, system, or role associated with that key, and information authenticating both the key and the association between that identity and that public key. The keys used by PEM are one example of a key certificate [Kent93].

Passive Attack: An attack on an authentication system that inserts no data into the stream, but instead relies on being able to passively monitor information being sent between other

parties. This information could be used a later time in what appears to be a valid session. (See active attack and replay attack.)

Plain-text: Unencrypted text.

Replay Attack: An attack on an authentication system by recording and replaying previously sent valid messages (or parts of messages). Any constant authentication information, such as a password or electronically transmitted biometric data, can be recorded and used later to forge messages that appear to be authentic.

Symmetric Cryptography: An encryption system that uses the same key for encryption and decryption. Sometimes referred to as Secret˜Key˜Cryptography.

3. AUTHENTICATION TECHNOLOGIES

There are a number of different classes of authentication, ranging from no authentication to very strong authentication. Different authentication mechanisms are appropriate for addressing different kinds of authentication problems, so this is not a strict hierarchical ordering.

3.1 No Authentication

For completeness, the simplest authentication system is not to have any. A non-networked PC in a private (secure) location is an example of where no authentication is acceptable. Another case is a stand-alone public workstation, such as "mail reading" workstations provided at some conferences, on which the data is not sensitive to disclosure or modification.

3.2 Authentication Mechanisms Vulnerable to Passive Attacks

The simple password check is by far the most common form of authentication. Simple authentication checks come in many forms: the key may be a password memorized by the user, it may be a physical or electronic item possessed by the user, or it may be a unique biological feature. Simple authentication systems are said to be "disclosing" because if the key is transmitted over a network it is disclosed to eavesdroppers. There have been widespread reports of successful passive attacks in the current Internet using already compromised machines to engage in passive attacks against additional machines [CERT94]. Disclosing authentication mechanisms are vulnerable to replay attacks. Access keys may be stored on the target system, in which case a

single breach in system security may gain access to all passwords. Alternatively, as on most systems, the data stored on the system can be enough to verify passwords but not to generate them.

3.3 Authentication Mechanisms Vulnerable to Active Attacks

Non-disclosing password systems have been designed to prevent replay attacks. Several systems have been invented to generate non-disclosing passwords. For example, the SecurID Card from Security Dynamics uses synchronized clocks for authentication information. The card generates a visual display and thus must be in the possession of the person seeking authentication. The S/Key (TM) authentication system developed at Bellcore generates multiple single use passwords from a single secret key [Haller94]. It does not use a physical token, so it is also suitable for machine-machine authentication. In addition there are challenge-response systems in which a device or computer program is used to generate a verifiable response from a non-repeating challenge. S/Key authentication does not require the storage of the user's secret key, which is an advantage when dealing with current untrustworthy computing systems. In its current form, the S/Key system is vulnerable to a dictionary attack on the secret password (pass phrase) which might have been poorly chosen. The Point-to-Point Protocol's CHAP challenge-response system is non-disclosing but only useful locally [LS92, Simpson93]. These systems vary in the sensitivity of the information stored in the authenticating host, and thus vary in the security requirements that must be placed on that host.

3.4 Authentication Mechanisms Not Vulnerable to Active Attacks

The growing use of networked computing environments has led to the need for stronger authentication. In open networks, many users can gain access to any information flowing over the network, and with additional effort, a user can send information that appears to come from another user.

More powerful authentication systems make use of the computation capability of the two authenticating parties. Authentication may be unidirectional, for example authenticating users to a host computer system, or it may be mutual in which case the entity logging in is assured of the identity of the host. Some authentication systems use cryptographic techniques and establish (as a part of the authentication process) a shared secret (e.g., session key) that can be used for further exchanges. For example, a user, after completion of the authentication process, might be granted an authorization ticket that can be used to obtain other services without further authentication. These authentication

systems might also provide confidentiality (using encryption) over insecure networks when required.

4. CRYPTOGRAPHY

Cryptographic mechanisms are widely used to provide authentication, either with or without confidentiality, in computer networks and internetworks. There are two basic kinds of cryptography and these are described in this section. A fundamental and recurring problem with cryptographic mechanisms is how to securely distribute keys to the communicating parties. Key distribution is addressed in Section 6 of this document.

4.1 Symmetric Cryptography

Symmetric Cryptography includes all systems that use the same key for encryption and decryption. Thus if anyone improperly obtains the key, they can both decrypt and read data encrypted using that key and also encrypt false data and make it appear to be valid. This means that knowledge of the key by an undesired third party fully compromises the confidentiality of the system. Therefore, the keys used need to be distributed securely, either by courier or perhaps by use of a key distribution protocol, of which the best known is perhaps that proposed by Needham and Schroeder [NS78, NS87]. The widely used Data Encryption Standard (DES) algorithm, that has been standardized for use to protect unclassified civilian US Government information, is perhaps the best known symmetric encryption algorithm [NBS77].

A well known system that addresses insecure open networks as a part of a computing environment is the Kerberos (TM) Authentication Service that was developed as part of Project Athena at MIT [SNS88, BM91, KN93]. Kerberos is based on Data Encryption Standard (DES) symmetric key encryption and uses a trusted (third party) host that knows the secret keys of all users and services, and thus can generate credentials that can be used by users and servers to prove their identities to other systems. As with any distributed authentication scheme, these credentials will be believed by any computer within the local administrative domain or realm. Hence, if a user’s password is disclosed, an attacker would be able to masquerade as that user on any system which trusts Kerberos. As the Kerberos server knows all secret keys, it must be physically secure. Kerberos session keys can be used to provide confidentiality between any entities that trust the key server.

4.2 Asymmetric Cryptography

In the late 1970s, a major breakthrough in cryptology led to the availability of Asymmetric Cryptography. This is different from Symmetric Cryptography because different keys are used for encryption and decryption, which greatly simplifies the key distribution problem. The best known asymmetric system is based on work by Rivest, Shamir, and Adleman and is often referred to as "RSA" after the authors' initials [RSA78].

SPX is an experimental system that overcomes the limitations of the trusted key distribution center of Kerberos by using RSA Public Key Cryptography [TA91]. SPX assumes a global hierarchy of certifying authorities at least one of which is trusted by each party. It uses digital signatures that consist of a token encrypted in the private key of the signing entity and that are validated using the appropriate public key. The public keys are believed to be correct as they are obtained under the signature of the trusted certification authority. Critical parts of the authentication exchange are encrypted in the public keys of the receivers, thus preventing a replay attack.

4.3 Cryptographic Checksums

Cryptographic checksums are one of the most useful near term tools for protocol designers. A cryptographic checksum or message integrity checksum (MIC) provides data integrity and authentication but not non-repudiation. For example, Secure SNMP and SNMPv2 both calculate a MD5 cryptographic checksum over a shared secret item of data and the information to be authenticated [Rivest92, GM93]. This serves to authenticate the data origin and is believed to be very difficult to forge. It does not authenticate that the data being sent is itself valid, only that it was actually sent by the party that claims to have sent it. Crytographic checksums can be used to provide relatively strong authentication and are particularly useful in host-to-host communications. The main implementation difficulty with cryptographic checksums is key distribution.

4.4 Digital Signatures

A digital signature is a cryptographic mechanism which is the electronic equivalent of a written signature. It serves to authenticate a piece of data as to the sender. A digital signature using asymmetric cryptography (Public Key) can also be useful in proving that data originated with a party even if the party denies having sent it; this property is called non-repudiation. A digital signature provides authentication without

confidentiality and without incurring some of the difficulties in full encryption. Digital signatures are being used with key certificates for Privacy Enhanced Mail [Linn93, Kent93, Balenson93, Kaliski93].

5. USER TO HOST AUTHENTICATION

There are a number of different approaches to authenticating users to remote or networked hosts. Two types of hazard are created by remote or networked access: First an intruder can eavesdrop on the network and obtain user ids and passwords for a later replay attack. Even the form of existing passwords provides a potential intruder with a head start in guessing new ones.

Currently, most systems use plain-text disclosing passwords sent over the network (typically using telnet or rlogin) from the user to the remote host [Anderson84, Kantor91]. This system does not provide adequate protection from replay attacks where an eavesdropper gains remote user ids and remote passwords.

5.1 Protection Against Passive Attack Is Necessary

Failure to use at least a non-disclosing password system means that unlimited access is unintentionally granted to anyone with physical access to the network. For example, anyone with physical access to the Ethernet cable can impersonate any user on that portion of the network. Thus, when one has plain-text disclosing passwords on an Ethernet, the primary security system is the guard at the door (if any exist). The same problem exists in other LAN technologies such as Token-Ring or FDDI. In some small internal Local Area Networks (LANs) it may be acceptable to take this risk, but it is an unacceptable risk in an Internet [CERT94].

The minimal defense against passive attacks, such as eavesdropping, is to use a non-disclosing password system. Such a system can be run from a dumb terminal or a simple communications program (e.g., Crosstalk or PROCOMM) that emulates a dumb terminal on a PC class computer. Using a stronger authentication system would certainly defend against passive attacks against remotely accessed systems, but at the cost of not being able to use simple terminals. It is reasonable to expect that the vendors of communications programs and non user-programmable terminals (such as X-Terminals) would build in non-disclosing password or stronger authentication systems if they were standardized or if a large market were offered. One of the advantages of Kerberos is that, if used properly, the user’s password never leaves the user’s workstation. Instead they are used to decrypt the user’s Kerberos tickets, which are themselves encrypted information which are sent

over the network to application servers.

5.2 Perimeter Defenses as Short Term Tool

Perimeter defenses are becoming more common. In these systems, the user first authenticates to an entity on an externally accessible portion of the network, possibly a "firewall" host on the Internet, using a non-disclosing password system. The user then uses a second system to authenticate to each host, or group of hosts, from which service is desired. This decouples the problem into two more easily handled situations.

There are several disadvantages to the perimeter defense, so it should be thought of as a short term solution. The gateway is not transparent at the IP level, so it must treat every service independently. The use of double authentication is, in general, difficult or impossible for computer-computer communication. End to end protocols, which are common on the connectionless Internet, could easily break. The perimeter defense must be tight and complete, because if it is broken, the inner defenses tend to be too weak to stop a potential intruder. For example, if disclosing passwords are used internally, these passwords can be learned by an external intruder (eavesdropping). If that intruder is able to penetrate the perimeter, the internal system is completely exposed. Finally, a perimeter defense may be open to compromise by internal users looking for shortcuts.

A frequent form of perimeter defense is the application relay. As these relays are protocol specific, the IP connectivity of the hosts inside the perimeter with the outside world is broken and part of the power of the Internet is lost.

An administrative advantage of the perimeter defense is that the number of machines that are on the perimeter and thus vulnerable to attack is small. These machines may be carefully checked for security hazards, but it is difficult (or impossible) to guarantee that the perimeter is leak-proof. The security of a perimeter defense is complicated as the gateway machines must pass some types of traffic such as electronic mail. Other network services such as the Network Time Protocol (NTP) and the File Transfer Protocol (FTP) may also be desirable [Mills92, PR85, Bishop]. Furthermore, the perimeter gateway system must be able to pass without bottleneck the entire traffic load for its security domain.

5.3 Protection Against Active Attacks Highly Desirable

In the foreseeable future, the use of stronger techniques will be required to protect against active attacks. Many corporate networks based on broadcast technology such as Ethernet probably need such techniques. To defend against an active attack, or to provide privacy, it is necessary to use a protocol with session encryption, for example Kerberos, or use an authentication mechanism that protects against replay attacks, perhaps using time stamps. In Kerberos, users obtain credentials from the Kerberos server and use them for authentication to obtain services from other computers on the network. The computing power of the local workstation can be used to decrypt credentials (using a key derived from the user-provided password) and store them until needed. If the security protocol relies on synchronized clocks, then NTPv3 might be useful because it distributes time amongst a large number of computers and is one of the few existing Internet protocols that includes authentication mechanisms [Bishop, Mills92].

Another approach to remotely accessible networks of computers is for all externally accessible machines to share a secret with the Kerberos KDC. In a sense, this makes these machines "servers" instead of general use workstations. This shared secret can then be used encrypt all communication between the two machines enabling the accessible workstation to relay authentication information to the KDC in a secure way.

Finally, workstations that are remotely accessible could use asymmetric cryptographic technology to encrypt communications. The workstation’s public key would be published and well known to all clients. A user could use the public key to encrypt a simple password and the remote system can decrypt the password to authenticate the user without risking disclosure of the password while it is in transit. A limitation of this workstation-oriented security is that it does not authenticate individual users only individual workstations. In some environments for example, government multi-level secure or compartmented mode workstations, user to user authentication and confidentiality is also needed.

6. KEY DISTRIBUTION & MANAGEMENT

The discussion thus far has periodically mentioned keys, either for encryption or for authentication (e.g., as input to a digital signature function). Key management is perhaps the hardest problem faced when seeking to provide authentication in large internetworks. Hence this section provides a very brief overview of key management technology that might be used.

The Needham & Schroeder protocol, which is used by Kerberos, relies on a central key server. In a large internetwork, there would need to be significant numbers of these key servers, at least one key server per administrative domain. There would also need to be mechanisms for separately administered key servers to cooperate in generating a session key for parties in different administrative domains. These are not impossible problems, but this approach clearly involves significant infrastructure changes.

Most public-key encryption algorithms are computationally expensive and so are not ideal for encrypting packets in a network. However, the asymmetric property makes them very useful for setup and exchange of symmetric session keys. In practice, the commercial sector probably uses asymmetric algorithms primarily for digital signatures and key exchange, but not for bulk data encryption. Both RSA and the Diffie-Hellman techniques can be used for this [DH76]. One advantage of using asymmetric techniques is that the central key server can be eliminated. The difference in key management techniques is perhaps the primary difference between Kerberos and SPX. Privacy Enhanced Mail has trusted key authorities use digital signatures to sign and authenticate the public keys of users [Kent93]. The result of this operation is a key certificates which contains the public key of some party and authentication that the public key in fact belongs to that party. Key certificates can be distributed in many ways. One way to distribute key certificates might be to add them to existing directory services, for example by extending the existing Domain Name System to hold each host’s the key certificate in a new record type.

For multicast sessions, key management is harder because the number of exchanges required by the widely used techniques is proportional to the number of participating parties. Thus there is a serious scaling problem with current published multicast key management techniques.

Finally, key management mechanisms described in the public literature have a long history of subtle flaws. There is ample evidence of this, even for well-known techniques such as the Needham & Schroeder protocol [NS78, NS87]. In some cases, subtle flaws have only become known after formal methods techniques were used in an attempt to verify the protocol. Hence, it is highly desirable that key management mechanisms be kept separate from authentication or encryption mechanisms as much as is possible. For example, it is probably better to have a key management protocol that is distinct from and does not depend upon another security protocol.

7. AUTHENTICATION OF NETWORK SERVICES

In addition to needing to authenticate users and hosts to each other, many network services need or could benefit from authentication. This section describes some approaches to authentication in protocols that are primarily host to host in orientation. As in the user to host authentication case, there are several techniques that might be considered.

The most common case at present is to not have any authentication support in the protocol. Bellovin and others have documented a number of cases where existing protocols can be used to attack a remote machine because there is no authentication in the protocols [Bellovin89].

Some protocols provide for disclosing passwords to be passed along with the protocol information. The original SNMP protocols used this method and a number of the routing protocols continue to use this method [Moy91, LR91, CFSD88]. This method is useful as a transitional aid to slightly increase security and might be appropriate when there is little risk in having a completely insecure protocol.

There are many protocols that need to support stronger authentication mechanisms. For example, there was widespread concern that SNMP needed stronger authentication than it originally had. This led to the publication of the Secure SNMP protocols which support optional authentication, using a digital signature mechanism, and optional confidentiality, using DES encryption. The digital signatures used in Secure SNMP are based on appending a cryptographic checksum to the SNMP information. The cryptographic checksum is computed using the MD5 algorithm and a secret shared between the communicating parties so is believed to be difficult to forge or invert.

Digital signature technology has evolved in recent years and should be considered for applications requiring authentication but not confidentiality. Digital signatures may use a single secret shared among two or more communicating parties or it might be based on asymmetric encryption technology. The former case would require the use of predetermined keys or the use of a secure key distribution protocol, such as that devised by Needham and Schroeder. In the latter case, the public keys would need to be distributed in an authenticated manner. If a general key distribution mechanism were available, support for optional digital signatures could be added to most protocols with little additional expense. Each protocol could address the key exchange and setup problem, but that might make adding support for digital signatures more complicated and effectively discourage protocol designers from adding digital

signature support.

For cases where both authentication and confidentiality are required on a host-to-host basis, session encryption could be employed using symmetric cryptography, asymmetric cryptography, or a combination of both. Use of the asymmetric cryptography simplifies key management. Each host would encrypt the information while in transit between hosts and the existing operating system mechanisms would provide protection within each host.

In some cases, possibly including electronic mail, it might be desirable to provide the security properties within the application itself in a manner that was truly user-to-user rather than being host-to-host. The Privacy Enhanced Mail (PEM) work is employing this approach [Linn93, Kent93, Balenson93, Kaliski93]. The recent IETF work on Common Authentication Technology might make it easier to implement a secure distributed or networked application through use of standard security programming interfaces [Linn93a].

8. FUTURE DIRECTIONS

Systems are moving towards the cryptographically stronger authentication mechanisms described earlier. This move has two implications for future systems. We can expect to see the introduction of non-disclosing authentication systems in the near term and eventually see more widespread use of public key crypto-systems. Session authentication, integrity, and privacy issues are growing in importance. As computer-to-computer communication becomes more important, protocols that provide simple human interfaces will become less important. This is not to say that human interfaces are unimportant; they are very important. It means that these interfaces are the responsibility of the applications, not the underlying protocol. Human interface design is beyond the scope of this memo.

The use of public key crypto-systems for user-to-host authentication simplifies many security issues, but unlike simple passwords, a public key cannot be memorized. As of this writing, public key sizes of at least 500 bits are commonly used in the commercial world. It is likely that larger key sizes will be used in the future. Thus, users might have to carry their private keys in some electrically readable form. The use of read-only storage, such as a floppy disk or a magnetic stripe card provides such storage, but it might require the user to trust their private keys to the reading device. Use of a smart card, a portable device containing both storage and program might be preferable. These devices have the potential to perform the authenticating operations without divulging the private key they contain. They can also interact with the user requiring a simpler form of authentication to "unlock" the card.

The use of public key crypto-systems for host-to-host authentication appears not to have the same key memorization problem as the user-to-host case does. A multiuser host can store its key(s) in space protected from users and obviate that problem. Single user inherently insecure systems, such as PCs and Macintoshes, remain difficult to handle but the smart card approach should also work for them.

If one considers existing symmetric algorithms to be 1-key techniques, and existing asymmetric algorithms such as RSA to be 2-key techniques, one might wonder whether N-key techniques will be developed in the future (i.e., for values of N larger than 2). If such N-key technology existed, it might be useful in creating scalable multicast key distribution protocols. There is work currently underway examining the possible use of the Core Based Tree (CBT) multicast routing technology to provide scalable multicast key distribution [BFC93].

The implications of this taxonomy are clear. Strong cryptographic authentication is needed in the near future for many protocols. Public key technology should be used when it is practical and cost-effective. In the short term, authentication mechanisms vulnerable to passive attack should be phased out in favour of stronger authentication mechanisms. Additional research is needed to develop improved key management technology and scalable multicast security mechanisms.

SECURITY CONSIDERATIONS

This entire memo discusses Security Considerations in that it discusses authentication technologies and needs.

ACKNOWLEDGEMENTS

This memo has benefited from review by and suggestions from the IETF's Common Authentication Technology (CAT) working group, chaired by John Linn, and from Marcus J. Ranum.

REFERENCES

[Anderson84] Anderson, B., "TACACS User Identification Telnet Option", RFC 927, BBN, December 1984.

[Balenson93] Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", RFC 1423, TIS, IAB IRTF PSRG, IETF PEM WG, February 1993.

[BFC93] Ballardie, A., Francis, P., and J. Crowcroft, "Core Based Trees (CBT) An Architecture for Scalable Inter-Domain Multicast Routing", Proceedings of ACM SIGCOMM93, ACM, San Franciso, CA, September 1993, pp. 85-95.

[Bellovin89] Bellovin, S., "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Vol. 19, No. 2, March 1989.

[Bellovin92] Bellovin, S., "There Be Dragons", Proceedings of the 3rd Usenix UNIX Security Symposium, Baltimore, MD, September 1992.

[Bellovin93] Bellovin, S., "Packets Found on an Internet", ACM Computer Communications Review, Vol. 23, No. 3, July 1993, pp. 26-31.

[BM91] Bellovin S., and M. Merritt, "Limitations of the Kerberos Authentication System", ACM Computer Communications Review, October 1990.

[Bishop] Bishop, M., "A Security Analysis of Version 2 of the Network Time Protocol NTP: A report to the Privacy & Security Research Group", Technical Report PCS-TR91-154, Department of Mathematics & Computer Science, Dartmouth College, Hanover, New Hampshire.

[CB94] Cheswick W., and S. Bellovin, "Chapter 10: An Evening with Berferd", Firewalls & Internet Security, Addison-Wesley, Reading, Massachusetts, 1994. ISBN 0-201-63357-4.

[CERT94] Computer Emergency Response Team, "Ongoing Network Monitoring Attacks", CERT Advisory CA-94:01, available by anonymous ftp from cert.sei.cmu.edu, 3 February 1994.

[CFSD88] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", RFC 1067, University of Tennessee at Knoxville, NYSERNet, Inc., Rensselaer Polytechnic Institute, Proteon, Inc., August 1988.

[DH76] Diffie W., and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Volume IT-11, November 1976, pp. 644-654.

[GM93] Galvin, J., and K. McCloghrie, "Security Protocols for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1446, Trusted Information Systems, Hughes LAN Systems, April 1993.

[Haller94] Haller, N., "The S/Key One-time Password System", Proceedings of the Symposium on Network & Distributed Systems Security, Internet Society, San Diego, CA, February 1994.

[Kaufman93] Kaufman, C., "Distributed Authentication Security Service (DASS)", RFC 1507, Digital Equipment Corporation, September 1993.

[Kaliski93] Kaliski, B., "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services", RFC 1424, RSA Laboratories, February 1993.

[Kantor91] Kantor, B., "BSD Rlogin", RFC 1258, Univ. of Calif San Diego, September 1991.

[Kent93] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", RFC 1422, BBN, IAB IRTF PSRG, IETF PEM, February 1993.

[KN93] Kohl, J., and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, Digital Equipment Corporation, USC/Information Sciences Institute, September 1993.

[Linn93] Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", RFC 1421, IAB IRTF PSRG, IETF PEM WG, February 1993.

[Linn93a] Linn, J., "Common Authentication Technology Overview", RFC 1511, Geer Zolot Associate, September 1993.

[LS92] Lloyd B., and W. Simpson, "PPP Authentication Protocols", RFC 1334, L&A, Daydreamer, October 1992.

[LR91] Lougheed K., and Y. Rekhter, "A Border Gateway protocol 3 (BGP-3)", RFC 1267, cisco Systems, T.J. Watson Research Center, IBM Corp., October 1991.

[Mills92] Mills, D., "Network Time Protocol (Version 3) - Specification, Implementation, and Analysis", RFC 1305, UDEL, March 1992.

[NBS77] National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standards Publication 46, Government Printing Office, Washington, DC, 1977.

[NS78] Needham, R., and M. Schroeder, "Using Encryption for Authentication in Large Networks of Computers", Communications of the ACM, Vol. 21, No. 12, December 1978.

[NS87] Needham, R., and M. Schroeder, "Authentication Revisited", ACM Operating Systems Review, Vol. 21, No. 1, 1987.

[PR85] Postel J., and J. Reynolds, "File Transfer Protocol", STD 9, RFC 959, USC/Information Sciences Institute, October 1985.

[Moy91] Moy, J., "OSPF Routing Protocol, Version 2", RFC 1247, Proteon, Inc., July 1991.

[RSA78] Rivest, R., Shamir, A., and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Crypto-systems", Communications of the ACM, Vol. 21, No. 2, February 1978.

[Rivest92] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992.

[Simpson93] Simpson, W., "The Point to Point Protocol", RFC 1548, Daydreamer, December 1993.

[SNS88] Steiner, J., Neuman, C., and J. Schiller, "Kerberos: "An Authentication Service for Open Network Systems", USENIX Conference Proceedings, Dallas, Texas, February 1988.

[Stoll90] Stoll, C., "The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage", Pocket Books, New York, NY, 1990.

[TA91] Tardo J., and K. Alagappan, "SPX: Global Authentication Using Public Key Certificates", Proceedings of the 1991 Symposium on Research in Security & Privacy, IEEE Computer Society, Los Amitos, California, 1991. pp.232-244.

AUTHORS' ADDRESSES

Neil Haller
Bell Communications Research
445 South Street -- MRE 2Q-280
Morristown, NJ 07962-1910

Phone: (201) 829-4478
EMail: nmh@thumper.bellcore.com

Randall Atkinson
Information Technology Division
Naval Research Laboratory
Washington, DC 20375-5320

Phone: (DSN) 354-8590
EMail: atkinson@itd.nrl.navy.mil