Security in Storage Management: The Standards Question

Dr. Bruce K. Haddon
Sun Microsystems, Inc.
500 Eldorado Boulevard, UBRM01-241
Broomfield, CO 80021-3400 U.S.A.
Bruce.Haddon@sun.com
tel +1 303/ 272 8418
fax +1 303/ 272 5011

Abstract

The IEEE Computer Society announced the approval of the world's first Storage System Standards were approved on June 21st, 2000 [1], for the IEEE Media Management System (MMS) describing its architecture, data model, core media management protocol, and drive management and library management protocols. Four standards were approved, 1244.1 [2], 1244.3 [3], 1244.4 [4], and 1244.5 [5]. Notable by its absence in this announcement was the standard IEEE 1244.2, the "Session Security, Authentication, Initialization Protocol" (SSAIP) [6].

The IEEE Storage Systems Standards Working Group (SSSWG) [7] has spent considerable discussion time arriving at an understanding of the requirements for security in the 1244 family of standards. This paper discusses some of the issues surrounding the evolution of the requirements as they are currently used in defining the standard 1244.2.

1 Architecture and Terminology

The IEEE Open Storage System Interconnection (OSSI) Reference Model defines the structure of a storage system: in particular, the components: *Physical Volume Library* (PVL, effectively a database of information on the ways to access storage volumes); Physical Volume Repository (PVR, the actual cartridges and the means of making them accessible); *Media Access Point* (MAP, the mechanism for reading from and writing data to a partition of a cartridge), and *Mover* (the mechanism for streaming data from one place to another). The IEEE Media Management System (MMS) defines functional equivalents of the PVL, PVR, MAP and Mover, as well as providing name and location services, plus providing for management and security. 1244 assumes that communications are performed over TCP/IP channels, and that data I/O channels are private to the data client and the MAP (drive).

The diagram on the next page shows the relationship of the components of the Media Management System. The Drive Manager (DM) implements the control functions of the Mover, and the Library Manager the control functions of the PVR. The Media Manager (MM) "core" implements the remaining functions of the PVL and PVR. In the MMS, holding the needed details in the one Persistent Store coordinates the information about volumes, cartridges, *etc.*

The DM is, in many cases, best implemented within the operating system that provides the data path to the corresponding drive. The DM ideally can enforce the access rules related to the cartridge currently mounted, and also perform functions such as label checking, as well as protecting labels from un-permitted overwriting.

LM's are commonly on processors dedicated to an automated library, or can be implemented as "user-mode" applications with dedicated access to the libraries controls.

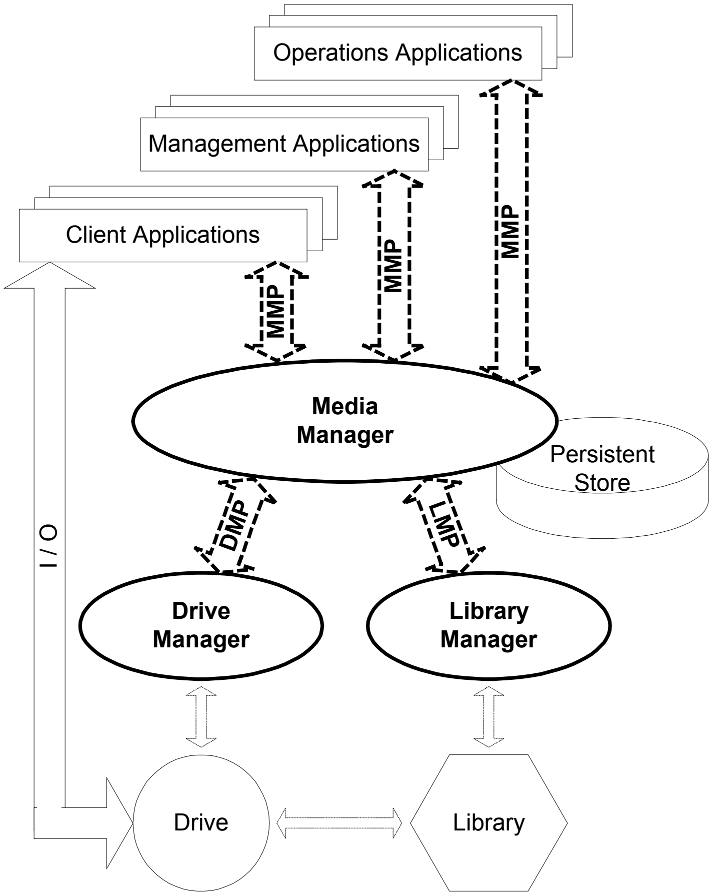

Figure 1 - The Components of the Media Management System

2 Security Background

The reason for the extended discussions is that the 1244.2 Standard has implications that go beyond the representation of management information and management operations. It defines the security environment in which management operations are performed, and management information is propagated.

The subject of 1244.2 is "security," *i.e.*, the questions of authentication (identifying who is requesting an operation), privacy (can anybody eavesdrop what is being done), and integrity (has anybody changed the information that is being exchanged).

The SSAIP has had a rocky history. The first version [8] circulated for balloting brought forth comments on its algorithmic completeness, encryption strength and hence accuracy of its authentication, and some questions about key management. These questions were addressed in a subsequent SSSWG meeting, but those discussions led only to further debate. A later proposal based the SSAIP on existing security-related standards, leading to a draft subsequently re-balloted as the document referenced as [9]

There are three operable features of security, as applied to storage management:

Authentication: (or *identification*), with its related subject of authorization, is assurance that another party to an interaction is, in fact, who they claim to be.

When a person purporting to be a police office comes to your door, authentication is requesting by asking for a form of identification, by which is meant that something “authentic,” *e.g.*, a police shield, should be presented. Once assured that the claim to identity is authenticated, a certain level of authorization is granted.

In some systems, authentication is followed by a request from one or both parties to be authorized in some role, but, as often as not, the level of authorization is implicit in the identification, *e.g.*, logging into a UNIX® system as *root*.

Privacy: the protection of data, either stored or in transit, from unauthorized “eavesdropping.” Ideally, privacy would also include protection of the identities of the parties communicating, and, even more idealistically, hide that the parties are communicating at all.

In everyday practice, that certain parties are communicating is not usually protected; a worker in his boss’s office is known to be there and communicating, only the content of the communication is protected by the closed door.

In general, the same is true of internetworking (including the Internet). IP packets carry interpretable addressing information, hence who is talking to whom, and when, it frequently available. The content of the packet may be encrypted to protect the content of the communication.

Integrity: is the protection of the data from interference, so that the message received is the same as, and all of, the message transmitted, and preferably, allows checking that the message genuinely came from the party claiming to have sent the message, and is the party that was previously identified.

In everyday usage, a number of mechanisms play an implicit role in “integrity.” In telephone conversations, fidelity must be sufficient to recognize the features of a person’s voice, and then, further, we rely on the redundancy of natural language (about 4 – 5 bits per word, *i.e.*, a density of about 10 – 15%) to notify or correct errors in transmission and reception. One of the tools for the computer era is the

> "message digest," a combination of encryption and trapdoor function that cannot be replicated unless the message is an unaltered message from the claimed source.

In the security arena, there have been many cases of "unbreakable" security being broken. There is not only the problem of incorrect implementation of secure constructs, but, in particular, many encryption or trapdoor algorithms have proven to be less resistant than originally believed [10]. Finally, a "security" mechanism is eventually no better than its support environment (*e.g.*, a password is no protection, if written on a piece of paper and attached to the computer's monitor).

In the area of encryption, the key distribution process is often one of the weaker links in the strength and safety of the overall encryption use.

The importance of the role of security in storage system management is illustrated by the central position of the support of security mechanisms in the Federated Management Architecture [11], on which the Jiro™ technology is built [12].

3 IEEE Standards Process

The IEEE standards process puts proposed standards to an interested group of volunteer balloters. After responses, a "Ballot Review Committee" (in this case, a subcommittee of the SSSWG) answers any questions. The history of 1244.2 is that the responses to the first round of review requested more information on which the effectiveness of the SSAIP could be evaluated.

The information requested after the first round of the balloting of 1244.2 essentially asked for specification of the algorithms which were to be used for encryption and message signing, as well as some implied questions about key distribution.

Because of these comments, and discussion within the SSSWG, a proposal was made to undertake a different approach. This approach is described later in this paper.

The revised 1244.2 document was then re-circulated to the IEEE balloters for further appraisal. No further comments arose out of doubts about the effectiveness of the security mechanisms proposed. There was a questioning of the little time permitted for public comment on the new document [6]. It is true that the process of the generating the new document used the approved methods of the SSSWG for "offline" interchange and discussion (email), and consequently was accomplished between scheduled meetings. Yet after evaluation of the objections, which did happen at a scheduled meeting, it was decided to keep the content of the document unchanged from the version defined in [6]. After other editorial changes, the document was re-issued as [13].

4 The Requirements

A result of the comments raised on the first circulation of 1244.2 was a re-examination of the requirements of "security" in the MMS [14]. The new requirements were:

1. “Security” is not an add-on feature in software or computer installations, so the security mechanisms of the MMS must mesh with those of the host systems (including the option of having no security additional to the host system).

Security exists only when the security fabric is unbroken at all accessible points. Hence, the SSAIP must not only be a part of the MMS, but it must also integrate into the overall operations and management of systems needing media management. The issues of 1244.2 are the issues of all computer systems that include media and media management.

2. Security infrastructure must be trusted

Security, in all its forms, is based on trust, and trust relationships. The nature and extent of trust relationships is not usually fully appreciated. It two people share, say, an apartment, and both have keys to the front door, one has to trust the other not to distribute additional copies of the key. Moreover, if such distribution is necessary, ideally there will be mechanism to trace the copy to its source. Should a trust relationship dissolve, then there needs also to be some method of revoking the trust. In the house key example, revocation is the act of changing the locks. All outstanding keys, trusted or not, are then useless. This is yet another example of the connection between security, and the environment in which it exists.

3. The IEEE SSSWG is not a creator, maintainer, validating agency, or clearance house of security concerns.

As noted earlier, it is the nature of security methodologies that, over time, problems will be found with the theory, the implementations, the ways in which otherwise perfectly good methods are used in specific circumstances, and the defined processes for distributing the software, the keys, as well as attacks on the infrastructure. Dealing with such problems is a full-time industry for some companies other watchdog agencies [15]. The SSSWG could not see, as a *working* group, that it would have either the time and expertise, or be able to commit to such an ongoing task, in any effective manner. It was also beyond the charter of the SSSWG to delegate such a task to another body.

The first SSAIP version was committing the IEEE SSSWG to establishing, and maintaining, cryptographic protocols of the strength of SSL3, and its possible successors. It may have also been committing the SSSWG to creating a mechanism for “webs of trust” in parallel to the technology established by the use of X.509 certificates. Because of the unanswered concerns with getting involved in such pervasive and complex matters, the earlier versions of the SSAIP, including those that only existed for intermediate discussion, must be regarded as being incomplete.

4. Media management and media access will be performed over public and semi-public networks.

Media management and access will live within the framework of the public Internet. Security has to be strong enough to survive the attacks that can be mounted in that environment.

It is a prediction for the future of automated libraries that such features at HTTP-based systems management, as well as LM functions, will become commonplace, and that such features will be seen as a competitive advantage by both suppliers and customers. The costs associated with enabling networked solutions will easily be absorbed into the market for such functions.

Some further indication of the direction in which the SSSWG believes storage technology is headed can be seen in the proposals made over the last several years for "Network Attached Storage" (NAS) [16]. In these proposals, disks are shared at the lowest level between computing systems, over networks. This is accomplished by digitally encrypting the disk positioning commands and the data that pass to and from the disks, not just to ensure privacy, but to provide each computing system with a virtual channel that may only be used by that system. This requires disks controllers to be able to support the software stacks for network protocols, authentication methodologies based on certificates or the near equivalent, and encryption and decryption at data transmission speeds. The epiphany comes when it is realized that these proposals have garnered high degrees of enthusiastic support from most segments of the storage industry. The proposed IEEE 1244 suite of standards, with its security measures defined by the proposed 1244.2 standard, places much lower demands on implementers of conforming products than any variant of the NAS proposals.

The Internet (including its various parts, and the underlying communications infrastructure) is the single most significant driver of information technologies on the planet today, and its use is growing exponentially, limited only by the rate at which communications bandwidth can be economically made available, and eventually, by the population of the planet (or perhaps, the occupied Universe).

There are already some, perhaps tentative, storage services being offered on the Internet. An MMS should be implementable using the Internet for communications, and it is essential that this principle should be used as a "litmus test" for discarding proposals that do not meet this objective. As the Internet undergoes further evolution in the direction of supporting real time communications (for telephone, streaming video, TV enhancement and replacement; all established directions), the movement of data for storage purposes will become increasingly commonplace.

5 The Two Balloted Proposals

5.1 The Previous Scheme

The first balloted version of the SSAIP provided a **password** protocol and an **md5/1.0** protocol, and optionally allowed other protocols to be supported. The **password** protocol used clear-text password authentication. It allowed a MM server to authenticate a client in a lightweight and insecure manner, similar to a login and password being transmitted as part of a *telnet* or *ftp* session.

The **md5/1.0** protocol proposed the use of the MD5 [10] one-way cryptographic hash, a random number exchange, and a shared secret (stored, common password) to implement client-server authentication and message integrity checking for all subsequent messages sent *via* the TCP connection during the session. The first part of the protocol had the client and server exchange a pair of random numbers that would be used during the session. The first part of the protocol determined two random values, *r1* and *r2*, which were to be used to compute a unique session key for the session. The session key was computed by concatenating the string values of *r1*, *r2*, and the shared secret (password) that is known to both the client and the server. That concatenated string is then hashed using the MD5 algorithm, producing a 32-byte value: The use of a shared password, and the concatenated values, could effectively ensure the integrity of a message between the MM and the client.

5.2 The Current Scheme

In the second version of the SSAIP, authentication was proposed to be absent, or be *via* a password, or *via* X.509 [17] certificates.

The password scheme is essentially the same as that proposed in the earlier version, but allowed the client to also insist upon a password from the MM server, so that the client and the MM server, even at this lower level of security, could authenticate each other.

The higher level of authentication is based on X.509 certificates, and thus the use of public key encryption, and the "web of trust" that certificate authorities can create. At this level, certificates rather that simple passwords are exchanged, and the content of the certificates is used to perform the authentication.

It is also permitted that client and server by-pass any authentication, and simply identify each other by name.

Privacy and integrity are, in the revised SSAIP, proposed to be based on the secure socket layer (SSL) [18]. To accomplish this, an MM server that supports SSL would also listen for communications on a second IP port. Communications on this port are established in a manner exactly similar to way a browser establishes connection over SSL when using the HTTPS protocol. The result is a TCP/IP session that is encrypted. The TCP sum-checks and sequence numbers cannot be "faked" without cracking the encryption, nor can the contents be interpreted.

The current state of SSL allows the use of 128 bit encryption—essentially unbreakable using current technology. Thus, the use of SSL ensures both privacy, and integrity.

All the balloters objecting to the first published version of the SSAIP expressed their satisfaction with the change, but new objections were registered, suggesting that the new proposal committed implementers to heavy code or coding demands in order to provide X.509 and SSL.

6 Issues

6.1 The SSL Implementation Burden

A concern was that the new scheme places unnecessarily burdensome requirements on those writing MMS components, particularly those who are expecting to put them in embedded systems such as library controllers.

The concern for "implementability" is well placed, and is a concern that played a part in shaping the proposed IEEE 1244.2 standard as it is currently written. However, implementing SSL is enabled by the OpenSSL library implementation of SSL3, which is freely available worldwide [19]. It is licensed under an Open Source license, one that allows commercial use of the software. The only relevant license requirement is that attribution for the SSL code be given in the documentation for the resulting product.

The SSL patents expired last year (2000), so it is anticipated that there will no further patent or export control problems with SSL. Other sources of such code include the Java™ Cryptographic Extension [20]. It is expected that the firmware associated with operating the drives attached to libraries constitutes a far more significant amount of code, and of testing, than the code associated with the SSL implementation.

Of the three MMS components, the "core" MM, the DM, and the LM, it is the DM and the LM that are candidates for embedding. The expectation is that DM's will remain host-based software for the near future; hence code size is not an overwhelming issue. DM's have to interact with the host tape driver software and "/dev" nodes. There is a required technology shift before DM's can leave the host.

In the near term, the LM's are the components most likely to be embedded into the library controller firmware. LM's may need all of authentication, privacy and integrity in establishing and conducting their communications. However, this is very likely only in the case of a shared library, which is being shared *via* a public or semi-public network. In most "computing center" uses, current practice will continue, which is the use of a dedicated connection (point-to-point network) between the controlling software (the MM in the proposed IEEE 1244 terminology) and the library. In this case, minimal identification authentication is needed, and privacy and integrity can be guaranteed by physical protection of the wire that is the direct connection.

A quick census has been made of some of the firmware images for manufacturer's current libraries, and they were found to be between 0.5 and 1.5 megabytes. It is not uncommon, however, for newer libraries to have two, four, or even 8 MB of flash memory, and even more RAM with which to work. Often, most of that is already allocated, but it expected that for newer generation libraries adding an implementation of SSL to library controller firmware, together with the required code to implement the LM components, would not be that difficult. Estimates indicate that the addition of SSL3 will add less than a further one-megabyte to these firmware components.

It should be kept in mind that the proposed IEEE 1244.2 standard does not require all implementations to include SSL facilities. It is expected that SSL3 will be offered only with higher end implementations, and in only those that offer media management over publicly, or at least, very widely, accessible networks.

At the instigation of a ballot response to the second balloting, an alternative to the use of SSL that was considered was using Virtual Private Networks (VPN), or socket forwarding *via* ***ssh***—since neither of these alternatives would require mechanisms inside the MMS standard. However, these mechanisms are general mechanisms for providing virtual extensions of private networks, using the Internet, or similar communications facilities, as communications media. These mechanisms essentially allow a private organization to reach other parts of the (communicating) world, and remain "private." This is not the same as offering "privacy" on the public network. (It is essentially the same difference as using a private point-to-point connection, and using techniques to ensure privacy while communicating on, say, a shared, broadcast media.)

There is no doubt that the currently circulated version of the proposed IEEE 1244.2 standard answered the required technical responses from the first round. It is also true that the most recently circulated version has been available for discussion within the IEEE Storage Systems Standard Working Group both before circulation and by means of the email reflector. This latter method of communicating had been decided upon by the SSSWG in general meeting as fulfilling the needs of discussing proposals. The most recent 1244.2 has also been discussed in face-to-face meetings since that circulation. No submissions have been made to those meetings to raise further objections.

6.2 The X.509 Communications Burden

By themselves, X.509 certificates require no more computational work than was proposed to the support the MD5 proposal. Extra work is required, in the form of having available communications to the certification authority, only if immediate checking of revocation is required. For services over the Internet, the communication channel will be available. In small, closed networks, this level of authentication is not required. In larger closed networks, it is anticipated that MMS suppliers will provide for the MM server itself to be the certification authority. In fact, many larger corporations and other similar organizations are already supporting their own certification servers.

6.3 The Dependency of IEEE Standards on Other Standards

This new version of the SSAIP makes the 1244 family of standards dependent upon the X.509 standard (and ISO standard) and SSL3 (an IETF RFC). However, of course, there are dependencies on ASCII, Unicode, TCP/IP, and others. Interdependency of standards is not in itself a bad thing, and, done correctly, is to be encouraged as a form of "re-use".

The IEEE SSSWG members agreed that it is the group's distinct intention that the entirety of the proposed IEEE 1244 standards suite should build in the most constructive manner on other standards, rather than attempt to establish variations in practice in areas that are not of specialized concern to the management of media.

7 Future Work

7.1 The Question of the Middle Ground

The SSAIP as now defined has options for no authentication, authentication by passwords, and authentication by means of X.509 certificates. A client can select no privacy and the integrity of just TCP/IP, or privacy and integrity provided by SSL3 encryption. The question has been raised of a "middle ground," *i.e.*, authentication stronger than unencrypted passwords but requiring less mechanism than X.509, and encryption for privacy and integrity requiring less support than SSL3.

This concept of a middle ground has been discussed in email exchanges, and again at the more recent meetings of the SSSWG. The concept has garnered general support in principle from members of the SSSWG, while still proving very elusive in terms of precise definition. It is attractive to postulate that there be a 1244.2-friendly protocol and methodology that is simple, free of administrative and communications overhead, and as secure as SSL.

A simple scheme was developed and implemented as part of Silicon Graphic's OpenVault [21], which would be applicable to the current form of the MMS. This scheme would completely cover this "middle ground" where MMS's could operate—between the totally insecure environment of clear-text passwords and the high-security SSL/Certificate scheme proposed by the latest 1244.2.

However, as noted before, the SSSWG also identified the overhead that it, or an ongoing organization, would have to undertake to deal with responses to threats as they were discovered. A further implication is that the 1244 family would have to be extended to define a network layer through which all MMS modules would have to communicate (just as SSL3 is a common layer).

The further difficulty is that although the "middle ground" concept is technologically attractive, it must be observed that there exist no (commercial or otherwise) off-the-shelf solutions fitting these characteristics. This observation implies either (or both of), a) that the solution is not so easy that is has been described publicly, or b) that there is insufficient demand to inspire publication or production of such a solution.

Still, there is no evidence that such a "middle ground" cannot be developed. It is also evident that should such a solution be developed, it can be made consistent and compatible with the current proposed IEEE 1244.2 framework. It is reasonable that the current version should continue to move through the balloting process, with no prejudice against a later extension or revision adding the "middle ground," should the development work be successful and the demand eventuate.

7.2 Extension and Revision

As much as the user community might like "standards" to stand immutably, the truth is that they are living, changing documents, since experience is a tough, but thorough, teacher. Even a standard as uncontroversial as ASCII [22] has been through three distinct revisions since it was first issued.

The future work with regard to the SSAIP, and the other IEEE 1244.2 Standards, will consist of continuing to work with balloters to answer their questions and objections, undertake real implementations to further test the concepts, and to continue such thought work as identifying and defining “middle ground” solutions. 1244.2 will be revisited, the requirements refined, to meet the needs of the storage using community.

8 Conclusions

There is no simple answer to the provision of security in computer systems, and particularly, in the security of management in computer systems.

Each of the aspects, authentication, privacy, and integrity, has its place, and each is orthogonal to the others. The current proposal provides for the strongest protection using available and tested techniques. Further, since these techniques have other uses, they will continue to be strengthened as overall experience dictates.

Nevertheless, the ability to create smaller, simpler implementations has not been lost. “Home libraries” at a reasonable cost are possible, where protection is not required.

Should the need for other levels of protection be proven, the structure of the SSAIP as embodied in the current version of IEEE 1244.2 allows for extension without removing any of the current protection.

Acknowledgements

The work that goes into standards is committee work, and, over time, particularly as long a time as the life of the SSSWG, many people are involved, and some contribute more than others. However, given that all participate voluntarily, and are supported by many companies and other institutions, it is inappropriate to single out individuals. They know who they are. The author recognizes that the Storage System Standards Working Group is the forum in which the matters discussed here developed and were resolved, and thanks it, collectively, for the opportunity to have written about these issues.

Final Note

P1244.2 was approved as a new standard by the IEEE-SA Standards Board on 7 December, 2000.

References

(Some SSSWG documents are "members only:" contact the SSSWG Chair as posted on the Web site to arrange member status for these documents.)

[1] IEEE Computer Society: *Press Release*, Washington, D.C. 18 July, 2000.

[2] *Approved Draft*: **1244.1-2000 IEEE Standard for Media Management System (MMS) Architecture**. *Print:* 140 pages [0-7381-2541-5] (2000)**.**

[3] *Approved Draft*: **1244.3-2000 IEEE Standard for Media Management System (MMS) Media Management Protocol (MMP)**. *Print:* 92 pages [0-7381-2539-3] (2000).

[4] *Approved Draft***: 1244.4-2000 IEEE Standard for Media Management System (MMS) Drive Management Protocol (DMP)**. *Print:* 40 pages [0-7381-2512-1] (2000).

[5] *Approved Draft*: **1244.5-2000 IEEE Standard for Media Management System (MMS) Library Management Protocol (LMP)**. *Print:* 34 pages [0-7381-2537-7] (2000)**.**

[6] *Unapproved Draft*: **1244.2 Draft Standard for Media Management System (MMS) Session Security, Authentication, Initialization Protocol (SSAIP)**. *Print:* 8 pages [0-7381-2577-6] (2000)**.**

[7] SSSWG: **The SSSWG home page**. http://www.ssswg.org/.

[8] Peck, Geoffrey G. (Ed.): **IEEE 1244.2/032000: Draft Standard for Media Management System (MMS): Session Security, Authentication, Initialization Protocol (SSAIP)**. **http://www.ssswg.org/membersonly/older/P1244.2.032000.doc**. (1999).

[9] Klier, Jan (Ed.): **IEEE 1244.2/041900: Draft Standard for Media Management System (MMS): Session Security, Authentication, Initialization Protocol (SSAIP)**, **http://www.ssswg.org/membersonly/latest/P1244.2.041900.doc**. (2000).

[10] Schneier, Bruce: **Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C**. John Wiley and Sons, Inc., New York (1996). ISBN 0-471-12845-7.

[11] Connor, William, PhD: **Federated Management Architecture (FMA) Specification, v1.0**. **http://java.sun.com/aboutJava/communityprocess/final/jsr009/index.html**, Sun Microsystems, Inc. (January, 2000).

[12] ***Jiro Technology***: **http://www.jiro.com/**. Sun Microsystems, Inc.

[13] Haddon, Bruce K. (Ed.): **IEEE 1244.2/TBD: Draft Standard for Media Management System (MMS): Session Security, Authentication, Initialization Protocol (SSAIP)**. (2000).

[14] IEEE Storage Systems Standards Working Group: **IEEE Media Management System (MMS) Requirements Document (DRAFT), Version 5.2**, **http://www.ssswg.org/public_documents/MMS_REQ_draft5.2.html** (January, 1998)

[15] Carnegie Mellon Software Engineering Institute: **Computer Emergency Response Team (CERT) Coordination Center**. **http://www.cert.org/**.

[16] Gibson, G. A., Van Meter, R.: “Network Attached Storage Architecture,” CACM, Vol. 43, No 11 (November, 2000).

[17] Consultation Committee, International Telephone and Telegraph (CCITT): “Recommendation X509: The Directory—Authentication Framework.” International Telecommunications Union, Geneva (1989).

[18] Internet Engineering Task Force (IETF): **The SSL Protocol, Version 3.0. Internet Draft**, http://www.netscape.com/eng/ssl3/draft302.txt (November 18, 1996).

[19] ***OpenSSL***: **http://www.openssl.org/**.

[20] ***Java Cryptography Extension 1.2***: **http://java.sun.com/products/jce/index-12.html**. Sun Microsystems, Inc.

[21] ***SGI OpenVault System Design***: **http://www.sgi.com/software/openvault/techspecs.html**. Silicon Graphics, Inc.

[22] ***ANSI-X3.4:*** **American Standard Code for Information Interchange**. American National Standards Institute, 1963, 1968, 1986, 1997.

Disclaimers and Notices

The opinions presented in this paper, except as noted, are those of the author, and do not necessarily agree with or reflect any matter of opinion or of policy of the IEEE, the SSSWG, or Sun Microsystems, Inc.

THIS PAPER AND ITS CONTENTS ARE PROVIDED WITHOUT ANY WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT WILL SUN BE LIABLE FOR ANY CLAIMS FOR DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF THIS PAPER OR ITS CONTENTS.

The technology and products described in this paper may be protected by one or more U.S. patents, foreign patents, and/or pending applications.