Endorsements, Licensing, and Insurance for Distributed System Services

Charlie Lai Gennady Medvinsky B. Clifford Neuman

Information Sciences Institute
University of Southern California

Abstract

Clients in a distributed system place their confidence in many servers, and servers themselves rely on other servers for file storage, authentication, authorization, and payment. When a system spans administrative boundaries it becomes harder to assess the security and competence of potential service providers. This paper examines the issue of confidence in large distributed systems.

When confidence is lacking in the "real world," one relies on endorsements, licensing, insurance, and surety bonds to compensate. We show that by incorporating such assurances into a distributed system, users are better able to evaluate the risks incurred when using a particular server. This paper describes a method to electronically represent endorsements, licenses, and insurance policies, and discusses the means by which clients use such items when selecting service providers.

1 Introduction

In distributed systems, local applications rely on remote servers to provide file storage, computation, authentication, authorization, and other functions. Such servers should be judged by their users, or user's organizations, to be secure and competent to perform the offered services. In smaller systems, users have confidence in service providers governed by the same administrative body to which they belong. When a system spans administrative boundaries, applications may rely on servers provided by other organizations. Users rarely understand the policies of remote organizations, making it hard to assess confidence in such foreign servers. Without sufficient assurance, users may limit their interactions to only those servers within their own administrative domain, limiting sharing – a principal benefit of a distributed system.

In the "real world" one relies on endorsements, licensing, liability insurance, and surety bonding to compensate for such lack of confidence. For example, the American Automobile Association provides endorsements for hotels and restaurants using a five-diamond scale, and the Better Business Bureau provides information about local businesses. In computer systems, these assurances can be represented by certificates digitally signed by the endorser, licensing authority, or insurance provider. Such *assurance credentials* would be granted to a server after it meets the requirements set by the organization issuing the credentials [7].

A *license* is a credential that indicates a service provider is legally authorized to provide a service. It indicates that the service provider has been found to meet certain minimal qualifications required by law, and that the service provider is subject to regulation and sanctions if found to be violating the law. The extent to which licensed service providers are monitored varies depending on the service, but is usually minimal. Licenses usually are issued by governmental bodies, are rarely revoked, and are on occasion obtained fraudulently. A license rarely provides information about the quality of a service.

An *endorsement* provides assurance that a service provider meets more rigorous requirements determined by the endorser, and usually provides information about the quality of a service provider, often as compared with other service providers. One's confidence in an endorsed service provider depends in part on one's confidence in its endorsers. In addition to services, endorsements may apply to products. For example, the Underwriters Laboratories endorses products as compliant with established safety standards.

While an endorsement or license assists in determining the level of risk involved in dealing with a service provider, a *liability insurance policy* or *surety bond* provides a client with a means to recover damages in the event of a loss that is the fault of the service provider.

When a user deals with an insured or bonded service provider, the risk of malfeasant or misfeasant behavior on the part of the service provider is partially shifted from the client to the insurance provider. Premiums for insurance are based on the level of risk assumed by the insurance provider. To be competitive, the parties insured may adopt policies that reduce this premium, potentially resulting in improved security for the distributed system as a whole.

This paper describes a method to electronically represent endorsements, licenses, and insurance policies, and discusses the means by which clients use such items when selecting service providers. We begin our discussion with the principles of liability insurance and surety bonding, which are the more general mechanisms described in this paper. Section 3 continues with a discussion of endorsements and licensing. The design of the system is presented in section 4. Server selection policies are described in section 5. In section 6, we discuss the implications of trusting insurance providers and endorsers themselves. The paper continues in section 7 by describing how the proposed mechanisms can improve confidence in several distributed system services and by discussing similarities with mechanisms already in use. The paper concludes with a brief summary.

Subject/Risk	G/S	Description of hazard or occurrence
AUTHENTICATION	General	Issue of improper credentials or disclosure of keys
SECURITY	General	Improper mediation of access
CURRENCY	General	Issue of unbacked currency (including counterfeit)
ACCOUNTING	General	Error in account maintenance, insufficient reserves
INSURANCE	General	Insufficient reserves to cover expected losses
STORAGE	General	Unauthorized disclosure of data, or loss of data
COMPUTATION	General	Unauthorized disclosure of data or computation, loss of integrity of computation
AVAILABILITY	Special	Failure to meet specified availability metric
ASSURANCE	Special	Failure to meet specified quality rating

Table 1: Common Hazards and Assurances

2 Liability Insurance

Today, three basic types of insurance exist: 1) personal insurance, which protects the life of the insured, 2) casualty insurance, which protects the property of the insured, and 3) liability insurance. Liability insurance does not cover personal losses of the insured; instead, the insured is covered for any legal obligation to pay damages inflicted upon a third party. Liability insurance providers agree to "assume loss or liability imposed by law with respect to certain property, rights, or liability caused by specified risks or hazards. The party to be insured against loss or liability is called the 'assured' or 'insured,' and the causes of damage, loss or liability are 'risks' or 'hazards'." [5]

A liability insurance contract is an agreement between an insurance provider and the insured. This contract, called a policy, specifies the obligations of the parties involved. The policy covers damages inflicted by the insured upon a third party if the damages were caused by an accident or occurrence. The words "accident" and "occurrence" do not include damages caused willfully by the insured. Liability insurance does not relieve the insured from responsibility for committing malicious acts. [5]

Surety bonding closely resembles liability insurance. The major distinction is that a liability insurance policy represents an agreement between two parties, and a surety bond represents an agreement among three parties: the surety, the obligee, and the principal. The surety (insurance provider) agrees to be responsible to the obligee (the party insured) for the conduct of the principal (the service provider). In other words, a surety bond guarantees to a prospective client the performance of a service provider. A surety bond also indemnifies the insured for any damages resulting from dishonest acts of the service provider. Unlike the coverage provided by liability insurance, these acts may be intentional or unintentional in nature. As a result, surety bonding provides greater coverage for clients than does liability insurance. [11]

Due to the similarities between surety bonding and liability insurance, we will use the term *insurance* to encompass both for the remainder of the paper.

When a policy is requested, insurance providers calculate the risk to be assumed by a liability insurance policy and fix the premium at an adequate level to reflect this risk. If the insured's situation or position changes, altering the assumed risk, the insurance provider has the right to alter the policy or charge a different premium [5]. Insurance providers will need to assess a service provider's procedures, past behavior, etc., to determine whether to insure the service provider and to set a premium.

Because issuing policies requires an assessment of the assumed risk, and settling claims requires judgement, neither of which are easily automated, we will leave such issues outside the system where they may be handled by the insurance agent, the adjustor, the injured party, and possibly the judicial system. In this paper, we concern ourselves with "proof of insurance", the mechanism by which users of a service verify that adequate coverage is in force.

Today, policies are written agreements certified by the signatures of the parties. In a computer system, the terms and the parties to such an agreement must be easily interpretable. For our purposes, the electronic representation of a policy will include the following information:

1. The names of the parties in a form suitable for authentication. Specifically:
   - The name of the insurance provider,
   - The name of the service provider,
   - A description of the obligee if a surety bond.
2. The subject of the insurance and the insured risks.
3. The period the policy is in force.
4. The limits of liability, possibly as:
   - An individual limit per occurrence or party,
   - An aggregate limit of liability,
   - Possibly zero (if endorsement or license).
5. Any other conditions pertaining to the insurance.

The standard representation of each of the elements of a policy is required so that applications can easily determine if the right kind of insurance is in place. For general coverages, the hazards insured against are determined by the category of the service provider. Several categories have been defined, including authentication, security, electronic currency, accounting/payment, data storage, and computation. The insured risks are standard for each of these service categories and are described in Table 1. Additional coverages may apply, e.g. service availability. Such "special" coverages have registered meaning, known to applications that require such coverage.

3 Licensing and Endorsements

Other mechanisms may be used to assess confidence in a service provider. For example, although prospective clients may not trust a service provider, confidence in the provider may be elevated through endorsements from trusted and well known organizations. Such organizations may officially endorse a service provider when they have found the service provider to be competent, trustworthy, and providing a high quality of service. Examples of organizations that issue endorsements today include the American Automobile Association, which provides endorsements for hotels and restaurants using a five-diamond scale, the Better Business Bureau, which provides information about local businesses, and the Underwriters Laboratories, which certifies that products

CERTIFICATE:	[Class:	Insurance, endorsement, or license
	Quota:	Limit of liability $1M (optional)
	Subject:	Currency (as per Table 1)
	Grantee:	CurrencyServer1
	Proxy Key:	$K_{Proxy}]K_{grantor}$
PROXY KEY:	K_{Proxy}	
GRANTOR:	Insurance agent, endorser, or license agent	

Figure 1: Assurance credential represented as proxy

meet certain safety standards. Endorsements do not provide compensation for damages incurred while interacting with service providers; instead they provide a mechanism for clients to better evaluate (and therefore reduce) the risk involved in dealing with service providers.

Similarly, users can require presentation of licenses from service providers proving the legal authority to offer a particular service. Issuance of a license might require a service provider to follow certain policies protecting its customers. In addition, before issuing a license, the licensing agency might verify that the party is competent to perform the service, as is done for licenses to practice medicine or law. Like endorsements, licensing does not provide compensation for damages, but it does provide prospective clients a simple means to reduce the likelihood of relying on illegitimate service providers.

The concept of an insurance policy, surety bonding, licensing, and endorsements are the same, differing solely in the limits and source of compensation in the event of a loss. Licensing usually provides no compensation by the licensing authority, endorsements provide no contractual liability on the part of the endorser (although they might be sued anyway), and insurance and surety bonding provide contractual liability by the insurance provider.

4 Implementation

The characteristics of insurance policies, endorsements, and licenses have already been described. To incorporate such mechanisms into a distributed system, we first define the basic representation of assurance credentials.

4.1 Representation of Assurance Credentials

An assurance credential can be an insurance policy, a surety bond, a license, or an endorsement. We represent such a credential as a restricted proxy [8]. A *proxy* is a token that enables one principal to operate with the privileges of another principal. A *restricted proxy* is a proxy that allows the exercise of such privileges for a particular purpose, subject to a specified set of conditions and restrictions. We use the term proxy in the remainder of this paper to mean a restricted proxy.

Figure 1 shows the proxy encoding of an assurance credential. When used to represent an assurance credential, the authority granted by a proxy is the right to assert that such an assurance is in force. The terms of the credential, i.e. the assurances provided, are encoded as restrictions, some of which are described in Table 1. The principal on whose authority a proxy is granted is referred to as the *grantor*. For assurance credentials this will be the insurer, the endorser, or the licensing agent. The proxy is signed by the grantor. This is represented abstractly in the figure by square brackets; the encryption keys used for the signature depend on the proxy implementation. The *grantee* or *delegate* is the principal to whom the proxy is issued, in this case the service provider. Although [8] calls the verifier of a proxy the *end-server*, such terminology is confusing here since the verifier of an assurance credential is the client of the service provider; consequently, we will use the term *verifier* instead.

Proxies can be divided into two classes: Bearer proxies and delegate proxies. Bearer proxies have an associated *proxy-key* that is used by the bearer to prove to the verifier possession of the proxy. To present a bearer proxy to the verifier, the grantee sends the certificate to the verifier and uses the proxy key to partake in an authentication exchange using the underlying authentication system. Delegate proxies have a list of delegates encoded as a restriction. They can only be used by one of the named delegates, which must send the certificate part of the proxy to the verifier and authenticate itself under its own identity. The verifier validates the certificate and checks to see that the delegate is included in the list of delegates. Both forms of proxies are suitable for representing assurance credentials.

Proxies may be implemented using either conventional or public-key cryptography. Both implementations are described in [8]. By defining assurance credentials as proxies, we free our mechanisms from dependence on a particular encryption algorithm. We also inherit the infrastructure needed to verify such credentials, and a structured framework within which the characteristics of the credential may be enumerated.

Service providers use proxies to demonstrate proof of insurance or endorsement. A client may request presentation of an assurance credential from a service provider, or may retrieve the credential from a separate directory service. Assurance credentials requested from the service provider may be bearer proxies, while those retrieved from a separate directory service must be delegate proxies.

4.2 Verification

When an assurance credential is received from a service provider or retrieved from a directory service, the client validates the credential in two steps. First, the proxy is verified cryptographically. The details of this verification will depend on the proxy mechanism used (e.g., public key vs. conventional cryptography, and bearer proxy vs. delegate proxy) and may require further interactions with other servers. Second, the restrictions, hazards, and assurances present in the proxy are extracted and compared against the user's and application's policy for server selection. Finally, the service provider must authenticate itself to the client using the underlying authentication protocol used by the system, possibly as part of a mutual authentication protocol in which the client and service provider prove their identities to one another.

Figure 2 shows the messages needed to retrieve and verify assurance credentials. Depending on the proxy mechanism used, some of the messages may be skipped. It is assumed that assurance credentials are issued to the grantee in advance, based on external agreements and evaluations by the grantor. It is further assumed that a client has settled on a candidate service provider and knows what assurances are required. In message 1, the client requests proof of assurance from the candidate service provider. The assurance is presented to the client in message 4 in a form that varies with different proxy implementations. Refer to [8] for details.

If the service provider requires a separate credential for each client (which will be the case in a conventional cryptography implementation), it requests and retrieves such a credential in messages 2 and 3. In such an implementation, the service provider sends a less specific credential to an authentication server, with the name of the prospective client.

Figure 2: Obtaining proof from service provider

The authentication server returns a new credential derived from the original one, encrypted in a key that may be verified by the client. Messages 2 and 3 will be absent in a public key implementation, possibly replaced by messages between the client and an authentication server to verify the public key of the grantor of the assurance.

After validating assurances from the service provider, clients may cache the assurance until its expiration, saving repeated requests on subsequent dealings with the same service provider.

4.3 Alternative Implementations

Alternative assurance mechanisms are possible. For example, one could require the client to contact the grantor of the assurance directly through an integrity protected channel. It is the concept of assurance that is important and the benefits of one implementation over another will depend on environmental assumptions including the real-time availability of insurers and endorsers.

5 Server Selection Requirements and Preferences

To utilize assurance credentials, distributed applications must be modified to request specific credentials, verify the credentials, and decide whether those credentials are sufficient according to a user specified server assurance policy. A user's server assurance policy identifies the assurances required for each class of application and identifies the assurance grantors whose assurances will be accepted. Usually a user's organization will provide a default configuration for use by its members. Users may extend the default settings, and may define their own configuration for non-business use. Such configuration information may be maintained in a configuration database, a distributed directory service, or a configuration file accessed by each application at run time.

The server assurance criteria will be different for different classes of applications. For example, banking servers may require proof of insurance issued by the FDIC, while insurance providers may require the combination of an endorsement by A.M. Best with a particular rating, and a license from the state insurance commissioner.

Because the server assurance criteria defines a subset of network servers with which a user can interact, it defines a custom view of the network. Information about the assurances available for each service provider could be stored in directory service entries for each service provider, making it easier for applications to choose candidates that meet the assurance criteria [9]. Similarly, some endorsers might provide directories of endorsed service providers making it even easier to identify candidate providers. Such directory service entries might be advisory only, with proof of assurance presented by the service provider as described in section 4.

6 A Framework for Building Confidence

Presence of assurance credentials should not by itself improve confidence in a service provider. The contribution of such credentials towards improving confidence in a service provider must depend in part on one's confidence in the endorser or insurance provider itself. There are many insurance companies, many organizations granting endorsements, and many jurisdictions issuing licenses. It is not practical to list all such assurance providers as part of each user's server assurance criteria. Instead, such criteria may identify organizations authorized to grant assurances for other assurance providers. For example, a user's server assurance criteria might require a service provider to present a business license from an agency with competent jurisdiction, of which only local agencies are listed directly; licenses for foreign license agencies may require assurance credentials for the licensing agency itself.

Such *transitive assurance* is common in the insurance industry. Insurance companies are rated and endorsed by agencies such as A.M. Best. In many jurisdictions, insurance companies must also be affiliated, with a portion of every premium dollar going to the jurisdiction to make good on claims with insurance companies that fail. This backing constitutes insurance of the insurance provider itself.

Transitive assurance may extend to an arbitrary depth, but longer chains generally promote less confidence. Where assurance is rated, heuristics are needed for deriving the combined assurance rating from the metrics and limits associated with the individual credentials involved. Such heuristics are a topic for further study.

Though confidence in an endorser or insurance provider is important, self-endorsement and self-insurance are also meaningful. Self-endorsement or self-insurance is analogous to marketing claims and warranties today. While such claims by a service provider might not instill as much confidence as outside endorsements and insurance, they can assist the user in differentiating between a production service and a prototype. They also allow a service provider to make claims regarding the efforts made to keep the service available.

As insurance, licensing, and endorsements are integrated with distributed system services, networks of assurance relationships will evolve. Figure 3 shows how such a network might appear. In the figure, dark arrows indicate a dependence on the correct operation of the destination of the arrow. Light arrows indicate that the source of the arrow will provide assurance for the service provider to which the arrow points. Dashed arrows indicate implied confidence.

In this example, client **C** requests service from service provider, **S2**. To provide this service **S2** subcontracts to service provider **S1**. **C**'s confidence in the composite service depends on the assurance provided for both **S1** and **S2**.

To improve customer confidence, **S1** and **S2** obtain a liability insurance policy from insurance provider **I1**. As long as **C** has confidence in *I1* this provides assurance that **C** will be compensated in the event of damages caused by **S1** or **S2**. In this example, **C** does not have confidence directly in the insurance provider, but will accept the endorsement of **E3**, an organization that rates insurance companies.

Figure 3: A network of trust relationships

Client **C** will also find that service providers **S1** and **S2** are licensed by licensing agency **L2**, indicating that **L2** has found each server competent in offering its services. The licensing authority **L2**, has not been endorsed directly, but is recognized as the appropriate licensing agency by **C**.

It is unlikely that the network of assurance relationships will be strictly hierarchical, though the network will contain components that are hierarchical. By not imposing a hierarchy, clients gain greater flexibility in specifying server selection policies.

7 Relationship to system services and other work

Users require confidence in the distributed system services they use. This section discusses some of these services, shows how assurance credentials affect confidence in the service provider and, in some cases, describes confidence mechanisms already used by the service.

7.1 Authentication

An authentication server certifies the association of encryption keys to individuals. The credentials issued by authentication servers are subsequently used to authenticate users to one another. In essence, an authentication server issues assurance credentials where the assurance provided pertains solely to the identity of the individual. Cross-realm authentication allows individuals registered with one authentication server to prove their identity to those registered with different authentication servers. Global cross-realm authentication is supported by several authentication systems [10, 12], and techniques for assessing confidence in foreign authentication servers has been discussed widely in the literature [1, 3, 4].

Most approaches require a hierarchical organization of realms, with trust relationships following the hierarchy. Assurance of the authority of an authentication server is provided by credentials issued by other servers in the hierarchy. A problem with the hierarchical organization of realms is that different administrative bodies with different policies control the authentication servers making it difficult to assess confidence in the authentication process as a whole.

In practice, it has been difficult to establish a complete hierarchy for authentication servers, precisely because the levels of confidence required for participating realms is not well understood, and organizations that have the stature to serve as realms near the root of the hierarchy are concerned about liability. Some systems, including Pretty Good Privacy (PGP) [13], loosen the requirements, allowing users to certify the keys of other users, avoiding the need for a complete hierarchy. Like the assurance mechanisms described in this paper, PGP users identify other users whose certifications they trust. Unlike endorsements, certifications in PGP pertain to identity only. Endorsements of the certification procedures of other users are not public.

Insurance, licensing, and endorsements, provide a better means to assess confidence in the certification policies of an intermediate realm. Insurance provides a means of recovering damages that result from faulty certifications, making individuals and other service providers more willing to rely on such certifications. The procedures of such authentication servers may be assessed by independent auditors, resulting in an endorsement that improves confidence by parties that trust the independent auditor.

7.2 Electronic Currency

Currency servers [2, 6] issue electronic currency and provide services for currency exchange. Currency servers for a distributed system will be governed by multiple administrative bodies and may exist in different jurisdictions. As with paper money, electronic currency should be backed, directly or indirectly, by real value. This backing is jeopardized by counterfeit currency, faulty accounting procedures, or fraud.

Today, paper currency is trusted because there are relatively few issuers, mostly sanctioned by national governments. There may be many more issuers of electronic currency, many of which will be less trusted. Users must be more cautious when dealing with electronic currency, and should not blindly trust unknown currency servers.

Using the assurance mechanisms described in this paper, backing of a currency may be represented by insurance with an aggregate liability limit equal to the amount of backing. The assurance credentials would be granted by the bank, accounting service, or any other body that maintains the assets backing the currency. The records and procedures of the currency server would be endorsed by independent auditors. These auditors can attest to the amount of currency in circulation and can verify that currency servers only issue properly backed currency.

7.3 Accounting

Accounting servers [8] maintain account balances for users, track consumption of resources, maintain quotas, and more generally act as electronic banks. The confidence of users in such services may be derived from insurance analogous to FDIC insurance of banks in the United States. The required level of assurance will depend in part on the kinds of balances maintained. A high level of assurance may be required for services that maintain large positive balances for its customers, while less assurance may be necessary for services that grant credit or maintain debit balances for customers (which are collected after the purchase service has been provided).

8 Status

Authentication credentials in version 5 of Kerberos provide preliminary support for restricted proxies. The assurance mechanisms described in this paper are not yet implemented. Work is underway to develop distributed accounting and currency services. The assurance mechanisms described in this paper are an important part of the implementation of those services.

9 Discussion and Conclusions

As a distributed system spans organizational boundaries and users interact more frequently with outside service providers, it becomes increasingly difficult to determine the appropriate level of confidence to place in the service provider. Without a method to assess the integrity and competence of service providers, sharing across organizations will be reduced. It is this sharing that is typically one of the strengths of a distributed system.

This paper examined the use of licensing, endorsements, and insurance as a mechanism for addressing this problem. The approaches are similar and may be implemented electronically as a single mechanism, but with different parameters. Together these approaches provide clients with several options for assessing confidence and evaluating the risks incurred when interacting with service providers. Clients may determine if a service provider has been endorsed by a respected organization, or if the service provider is licensed or insured. The degree of assurance required will differ from client to client, and from application to application.

Service providers will obtain insurance policies, surety bonds, licenses, and endorsements to offer prospective clients greater assurance in their ability to conduct their trade. With a financial incentive to improve the security and reliability of their systems, service providers will finally have a means to justify investment in security. With a basis for selecting service providers, users will finally have a means for choosing servers that can meet their operation and security requirements.

Acknowledgments

Steven Augart, Celeste Anderson, Sridhar Gullapalli, Shai Herzog, Katia Obraczka, Jon Postel, and Stuart Stubblebine provided discussion and comments on drafts of this paper.

References

[1] Andrew D. Birrell, Butler W. Lampson, Roger M. Needham, and Michael D. Schroeder. A global authentication service without global trust. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 223–230, April 1986.

[2] D. Chaum, A. Fiat, and N. Naor. Untraceable electronic cash. *Proceedings Crypto '88*, 1988.

[3] Virgil D. Gligor, Shyh-Wei Luan, and Joseph N. Pato. On inter-realm authentication in large distributed systems. In *Proceedings of the 1992 IEEE Symposium on Research in Security and Privacy*, May 1992.

[4] Butler W. Lampson, Martin Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4):265–310, November 1992.

[5] Rowland H. Long. *The Law of Liability Insurance*, volume 1 and 2, pages 1.2–13.7. Mathew Bender and Company, Inc., Oakland, California, 1992.

[6] Gennady Medvinsky and B. Clifford Neuman. Netcash: A design for practical electronic currency on the internet. In *Proceedings of the First ACM Conference on Computer and Communications Security*, November 1993.

[7] B. Clifford Neuman. Protection and security issues for future systems. In *Proceedings of the Workshop on Operating Systems of the 90s and Beyond*, pages 184–201. Springer-Verlag, July 1991. Lecture Notes in Computer Science #563.

[8] B. Clifford Neuman. Proxy-based authorization and accounting for distributed systems. In *Proceedings of the 13th International Conference on Distributed Computing Systems*, pages 283–291, May 1993.

[9] B. Clifford Neuman, Steven Seger Augart, and Shantaprasad Upasani. Using prospero to support integrated location-independent computing. In *Proceedings of the Usenix Symposium on Mobile and Location-Independent Computing*, August 1993.

[10] B. Clifford Neuman and Theodore Ts'o. Kerberos: An authentication service for computer networks. *IEEE Communications*, 32(9), September 1994.

[11] David Porter. *Fundamentals of Bonding, a Manual of Fidelity and Surety*, pages 9–11. The Rough Notes Co., Inc., Indianapolis, Indiana, 1970.

[12] Joseph J. Tardo and Kannan Alagappan. SPX: Global authentication using public key certificates. In *Proceedings of the IEEE Symposium on Security and Privacy*, May 1991.

[13] Philip Zimmermann. *PGP User's Guide*, volume 1 and 2. 1994. Distributed with PGP 2.6.

This research was supported in part by the Advanced Research Projects Agency under NASA Cooperative Agreement NCC-2-539 and other awards. The views and conclusions contained in this paper are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of any of the funding agencies. Figures and descriptions in this paper were provided by the authors and are used with permission.

The authors may be reached at USC/ISI, 4676 Admiralty Way, Marina del Rey, CA 90292-6695, USA. Telephone +1 (310) 822-1511, e-mail lai@isi.edu, ari@isi.edu, bcn@isi.edu.