Endorsements, Licensing, and Insurance for Electronic Commerce

The users of systems supporting electronic commerce rely on the service providers with which they transact business. Because such systems span multiple organizations, it is difficult for users to assess the security and competence of such service providers. This article looks at the issue of confidence in distributed systems. When confidence is lacking in traditional commerce, endorsements, licensing, liability insurance, and surety bonds are used to compensate. We show that by incorporating such assurances into distributed systems, users are better able to evaluate the risks incurred when using a particular service provider.

** by Charlie Lai and*
Dr. B. Clifford Neuman
University of Southern California

In electronic commerce, local applications rely on remote service providers to participate in electronic transactions. These service providers are typically judged by their users' organizations to be secure and competent to perform the offered services. At present, most electronic commerce is conducted between participants with external contacts and is governed by paper agreements outside the system. With such agreements in place, users have an existing means to assess confidence in service providers. As the conduct of electronic commerce increasingly occurs between parties that have no pre-existing relationships with one another, customers will have a harder time assessing the character and competence of service providers. In the 'real world' customers may rely on licensing, endorsements, liability insurance and surety bonding to compensate for such lack of confidence. For example, in the United States the Better Business Bureau provides information and assurances about local businesses to potential customers. In computer systems, such assurances can be represented as electronic certificates digitally signed by the licensing authority, endorser, or insurance provider. Such *assurance credentials* would be granted to a service provider after it meets the requirements set by the organization issuing the credentials [2]. Information describing the implementation of such credentials can be found in [1].

Assurance Credentials

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 regarding 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 upon one's confidence in its endorsers. In addition to services, products may also be endorsed. 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.

Reduction of Risk

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 transferred from the user to the insurance provider. Premiums for insurance are based on the level of risk assumed by the insurance provider. To be competitive, insured service providers may adopt policies to reduce this premium, potentially resulting in improved security for the distributed system as a whole.

The concept of a license, endorsement, insurance policy, and surety bond is 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.

To utilize assurance credentials, distributed applications must be modified to request and verify the credentials, and to also decide whether those credentials are sufficient to meet 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 from whom assurances will be accepted. Usually a users' 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 to be accessed by each application at run time.

Assurance Criteria

The server assurance criteria will be different for different classes of applications. For example, the use of a banking server may require proof of insurance issued by the FDIC, while acceptance of insurance credentials issued by an insurance provider may require the combination of an endorsement by A.M. Best with a particular rating, and a license from a governmental insurance commission.

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 user applications to choose servers that meet the assurance criteria [3]. Similarly, some endorsers might provide directories of endorsed service providers making it even easier to identify candidate providers.

Presence of assurance credentials should not by itself grant confidence in a service provider. The contribution of such credentials towards improving confidence 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.

Such *transitive assurance* is familiar from the insurance industry. Insurance companies are rated and endorsed by agencies such as A.M. Best. In many jurisdictions, insurance companies must be registered, and a portion of every premium dollar goes to a government fund to make good on claims with insurance companies that fail. This backing constitutes insurance for 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.

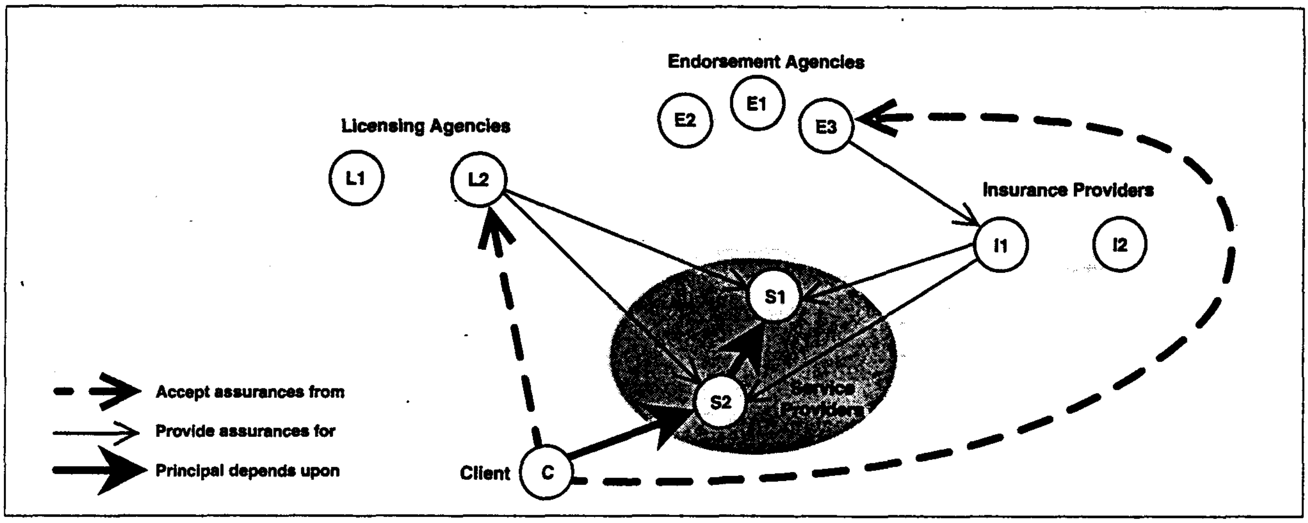

Figure 1: A network of trust relationships

Scenario

As licensing, endorsements and insurance are integrated with distributed system services, networks of assurance relationships will evolve. Figure 1 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 purchase 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. 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, although the network will contain components that are hierarchical. By not imposing a hierarchy, clients gain greater flexibility in specifying server selection policies.

Conclusion

This article examined the use of licensing, endorsements and insurance as several options for assessing confidence and evaluating the risks incurred when conducting electronic commerce with unfamiliar service providers. The approaches may be implemented electronically as a single mechanism, but with different parameters. The degree of assurance required will differ from client to client, and from application to application. Service providers will obtain licenses, endorsements, insurance policies, and surety bonds 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 have a means for choosing servers that can meet their operational and security requirements.

Acknowledgments

This article is based on a paper presented at the 2nd ACM Conference on Computer and Communications Security [1]. Gennady (Ari) Medvinsky contributed to the early design of the system described in this article. ■

References

[1] *Lai, C.; Medvinsky, G.; Neuman, B.C.:* Endorsements, Licensing, and Insurance for Distributed System Services, in: Proceedings of the Second ACM Conference on Computer and Communications Security, November 1994.

[2] *Neuman, B.C.:* Protection and Security Issues for Future Systems, in: Proceedings of the Workshop on Operating Systems of the 90s and Beyond, July 1991, pp 184-201.

[3] *Neuman, B.C.; Augart, S.; Upasani, S.:* Using Prospero to Support Integrated Location-independent Computing, in: Proceedings of the Usenix Symposium on Mobile and Location-independent Computing, August 1993.

** Charlie Lai (lai@isi.edu) is a Ph.D. student in the Computer Science Department at the University of Southern California. Dr. B. Clifford Neuman (bcn@isi.edu) is a scientist at the Information Sciences Institute and a faculty member in the Computer Science Department. He is one of the principal designers of the Kerberos authentication system. The work described in this article was supported in part by the Advanced Research Projects Agency through Ft. Huachuca under Contract No. DABT63-94-C-0034. The views and conclusions presented should not be interpreted as representing the official policies of the funding agencies. Figures and descriptions in this paper were provided by the authors and are used with permission.*