NRC·CNRC

NRC Publications Archive
Archives des publications du CNRC

An Agent Architecture for E-Service Privacy Policy Compliance

Yee, George; Korba, Larry

This publication could be one of several versions: author's original, accepted manuscript or the publisher's version. / La version de cette publication peut être l'une des suivantes : la version prépublication de l'auteur, la version acceptée du manuscrit ou la version de l'éditeur.

NRC Publications Record / Notice d'Archives des publications de CNRC:
https://nrc-publications.canada.ca/eng/view/object/?id=e0853fb2-70d6-450c-869b-299882e0530c
https://publications-cnrc.canada.ca/fra/voir/objet/?id=e0853fb2-70d6-450c-869b-299882e0530c

Access and use of this website and the material on it are subject to the Terms and Conditions set forth at
https://nrc-publications.canada.ca/eng/copyright
READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THIS WEBSITE.

L'accès à ce site Web et l'utilisation de son contenu sont assujettis aux conditions présentées dans le site
https://publications-cnrc.canada.ca/fra/droits
LISEZ CES CONDITIONS ATTENTIVEMENT AVANT D'UTILISER CE SITE WEB.

Questions? Contact the NRC Publications Archive team at PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca. If you wish to email the authors directly, please see the first page of the publication for their contact information.

Vous avez des questions? Nous pouvons vous aider. Pour communiquer directement avec un auteur, consultez la première page de la revue dans laquelle son article a été publié afin de trouver ses coordonnées. Si vous n'arrivez pas à les repérer, communiquez avec nous à PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca.

National Research Council Canada | Conseil national de recherches Canada

Canada

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

An Agent Architecture for E-Service Privacy Policy Compliance *

Yee, G., and Korba, L.
March 2005

* published in Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications (AINA 2005). Tamkang University, Taiwan. March 28-30, 2005. NRC 47431.

Copyright 2005 by
National Research Council of Canada

Permission is granted to quote short excerpts and to reproduce figures and tables from this report, provided that the source of such material is fully acknowledged.

Canada

An Agent Architecture for E-Services Privacy Policy Compliance[1]

George Yee and Larry Korba
Institute for Information Technology
National Research Council Canada
{George.Yee, Larry.Korba}@nrc-cnrc.gc.ca

Abstract

The growth of the Internet has been accompanied by the growth of e-services (e.g. e-commerce, e-health). This proliferation of e-services and the increasing regulatory and legal requirements for personal privacy have fueled the need to protect the personal privacy of e-service users. Approaches are needed to ensure that providers of e-services comply with the privacy policies of service users. In this paper, we examine privacy legislation to derive requirements for privacy policy compliance systems. We then propose an agent-based architecture for a privacy policy compliance system that satisfies many of the requirements and discuss the strengths and weaknesses of our proposed architecture.

1. Introduction

In order for e-services to be successful, privacy must be protected. An effective and flexible way of protecting privacy is to use privacy policies. Approaches for creating personal privacy policies are described in [1]. Privacy policy negotiation has been described in [2, 3]. In this work, we investigate the problem of privacy policy compliance. Given that the provider agrees to the consumer's privacy policy, how can the consumer be assured that the provider does indeed comply with the policy? A promising approach is to give the consumer control over her private information through the use of a Privacy Policy Compliance System (PPCS). In a previous paper [4], we derived the requirements for such a system and proposed a high-level architecture for a PPCS. In this paper, we refine our proposal and take the architecture closer to implementation by specializing on the use of agents.

Section 2 derives requirements for a PPCS by examining privacy legislation. Section 3 presents an agent-based architecture for a PPCS that satisfies many of the requirements of Section 2 and reviews related works in the literature. Section 4 gives our conclusions and plans for future work.

2. Requirements for PPCSs

To protect consumer privacy, many countries have enacted privacy legislation. In Canada, such legislation is enacted in the *Personal Information Protection and Electronic Documents Act (PIPEDA)* [5] and is based on the Canadian Standards Association's *Model Code for the Protection of Personal Information* [6], recognized as a national standard in 1996. This Code consists of ten Privacy Principles [6] that we call CSAPP. The CSAPP is representative of principles behind privacy legislation in many countries and so is a good source for privacy requirements for PPCSs.

In the following, CSAPP.n denotes Principle n of CSAPP. CSAPP.1, *Accountability*, says that a provider is "responsible for personal information under its control and shall designate an individual or individuals accountable for the organization's compliance with the privacy principles". This can be satisfied by the provider's PPCS clearly displaying the name(s) and contact information for the individual(s), called Privacy Compliance Officer(s), accountable for compliance. CSAPP.2, *Identifying Purposes*, says that the provider must identify the purposes for collecting personal information at or before the time the information is collected. CSAPP.3, *Consent*, says that the knowledge and consent of the consumer are needed for the "collection, use, or disclosure of personal information, except when inappropriate". These principles are automatically satisfied by the exchange of privacy policies between consumer and provider to see if their policies match (done prior to service engagement). For example, consider CSAPP.3. Since the consumer is in control of her privacy policy, the matching of this policy with the provider's privacy policy implies the consumer's knowledge and consent for the ensuing collection, use, and disclosure of the consumer's private information. Principles CSAPP.4, CSAPP.5, CSAPP.6, CSAPP.7, CSAPP.8, CSAPP.9, and CSAPP.10 are further requirements for the PPCS, as follows (we discuss CSAPP.7 at the end):

- *CSAPP.4, Limiting Collection:* for each purpose for which private information is collected, the PPCS must provide consumers with an explanation of what information is necessary in order to accomplish the purpose; this explanation must be open and retrievable by the general Internet community for scrutiny (to ensure that providers do not request information beyond what is necessary for the stated purpose); furthermore, for each purpose, the collection of private information must be securely logged and this log must be available to the owner of the private information or her designate for examination (to ensure that data is collected by fair and legal means).
- *CSAPP.5, Limiting Use, Disclosure, and Retention:* for each purpose for which private information is collected, the PPCS must provide consumers with an explanation of how it intends to use or disclose the consumer's private data; this explanation must be open and retrievable by the general Internet community for scrutiny; furthermore, for each purpose, the use and disclosure of the consumer's private data must be securely logged and this log must be available to the owner of the private data or her designate for examination and comparison against the previous explanation of use and disclosure (to ensure that providers do not use the consumer's private information for other than the stated purpose). In addition, the PPCS must ensure that all copies (including copies disclosed to other parties) of the consumer's private information are deleted at the earliest of a) the time when the data is no longer needed for the fulfillment of the purpose, or b) the expiration of the data's retention time. This deletion must also be securely logged and the log accessible by the owner of the private information or her designate.
- *CSAPP.6, Accuracy:* the PPCS must provide a facility with which consumers can access, check the accuracy, update, and add to their private data, as necessary for the corresponding purposes. These actions should also be securely logged and accessible to the provider or the data owner for verification purposes.
- *CSAPP.8, Openness:* upon request, the PPCS must display the provider's specific information about its policies and practices relating to the management of private information.
- *CSAPP.9, Individual Access:* upon a consumer's request, the PPCS must inform the consumer of the existence, use, and disclosure of her personal information, and give her access to that information; upon review of the information, the consumer can perform the actions of CSAPP.6.
- *CSAPP.10, Challenging Compliance:* upon request, the PPCS must allow the consumer or her designate to review the secure log to verify compliance to her privacy policy. In case of non-compliance, the consumer can take action outside the scope of the PPCS, i.e. notify the provider's Privacy Compliance Officer(s) of the non-compliance and take legal action if necessary.
- *CSAPP.7, Safeguards:* it is apparent from the above that the PPCS contains:
  a) the provider's explanations of what private data it requires for particular purposes,
  b) the provider's explanations of how it uses or discloses private data for particular purposes,
  c) the provider's specific information about its policies and practices relating to the management of private information, including the names and contact information for Privacy Compliance Officers,
  d) the provider's privacy policies,
  e) the consumer's privacy policies,
  f) the consumer's private data,
  g) the log entries.

  The PPCS needs to apply the following protection to these information groups: groups a), b), c), and d) can be viewed by anyone in the Internet community but need to be protected from unauthorized tampering; groups e) and f) must be viewable only by the provider, the party receiving the private information as a disclosure (view only the information disclosed and corresponding privacy policy), and the consumer owner of the private information; groups e) and f) can only be modified, deleted, or added-to by the consumer owner of the private information, except for deletion, where the provider or the party receiving the information as a disclosure can delete the information, either because the corresponding purpose has been accomplished, or the information's retention time has expired; group g) must be viewable only by the consumer owner of the corresponding private information, the consumer owner's designate, the provider, or the party receiving a disclosure of corresponding private information; group g) information once written by the PPCS, must not be modifiable by any party. Storage and transfer of the data referred to above will be access-controlled and use cryptographic techniques to protect data integrity and limit the release of the information. Moreover, the PPCS must assure authentication and authorization of service providers and consumers, and must resist attacks such as denial of service, man-in-the middle, code modification, and so on.

3. An agent architecture for PPCSs

Figure 1 presents the agent architecture for a PPCS that satisfies many of the requirements of Section 2. In Figure 1, the individual boxes within the PPCS house agents that act on behalf of the consumer (C-agents) or the provider (P-agents).

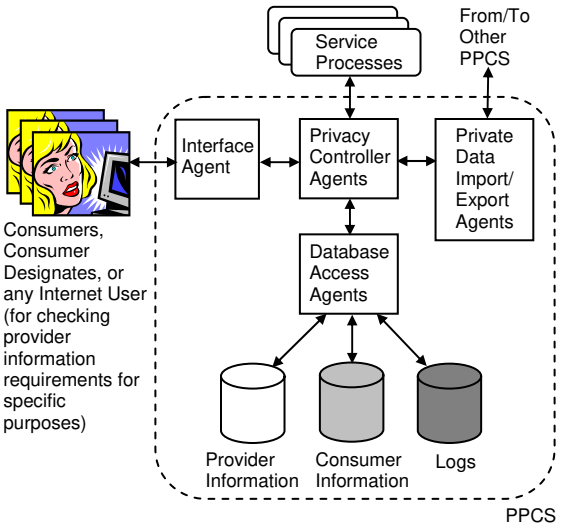

Figure 1. High-level PPCS architecture

Figure 2 shows the agents within each box. Descriptions of the PPCS agents in Figures 1 and 2 follow:

- *Interface C-agent:* handles interactions with the consumer, consumer designate, or any Internet user (for checking provider information requirements for specific purposes); specific actions include: a) provides interface for user access to update private information or to examine logs, b) upon request, displays provider information regarding names and contact information for Privacy Compliance Officers, provider specific policies on the management of private information, and provider explanations of what information is required for various purposes as well as how the private information will be used, c) establishes a secure channel to the consumer or consumer delegate and authenticates them (see Section 3.1).
- *Controller C-agent:* controls the flow of consumer information and requests to fulfill the PPCS Requirements (requirements of Section 2); specific actions include: a) grant access for the storage, retrieval, and update of consumer private information, b) grant access for the examination of logs and comparisons of information, c) upon request, inform the consumer of the existence, use, and disclosure of her private information (by reading logs). In addition, if the consumer updates private information that has been disclosed to other PPCSs, this agent passes the updates to those PPCSs via the Export C-agent.

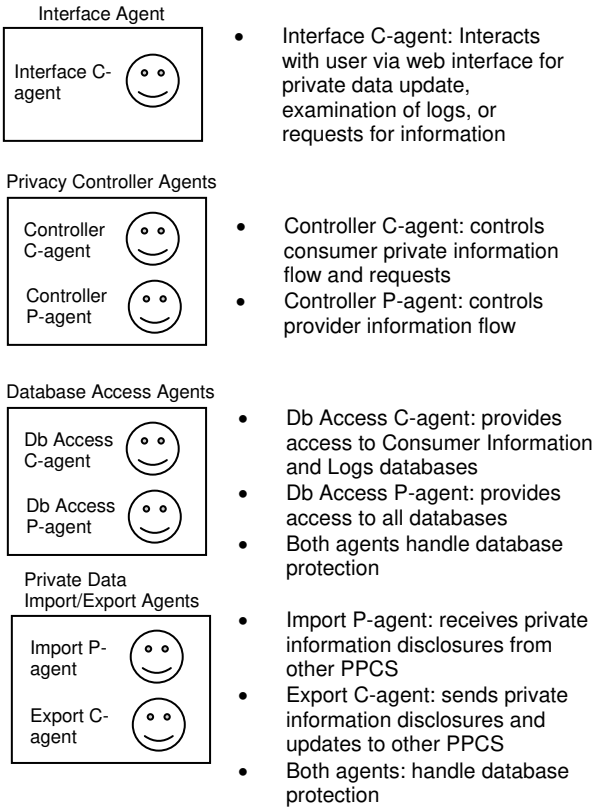

Figure 2. PPCS agents

- *Controller P-agent:* controls the flow of provider information to fulfill the PPCS Requirements; specific actions include: a) make log entries, b) delete private information upon completion of purpose or information expiry (expiry date retrieved from consumer's privacy policy in the Consumer Information database), c) channel the following to the Interface C-agent upon request: provider information regarding names and contact information for Privacy Compliance Officers, provider specific policies on the management of private information, and provider explanations of what information is required for various purposes as well as how the private information will be used, d) store/update the provider information in c) (this information is provided by a service process), e) channel private info to be disclosed to Export C-agent.
- *Db Access C-agent:* provides access to the databases as requested by the Controller C-agent; specifically, a) provides read/write access to the Consumer

Information database for the storage, retrieval, and update of consumer private information, b) provide read access to the Logs database for the examination of logs and comparisons of information (e.g. compare previously stated use); in addition, handles read/write protection for the Consumer Information database (see Section 3.1) to meet the requirements expressed in CSAPP.7.

- *Db Access P-agent:* provides access to the databases as requested by the Controller P-agent; specifically, a) provides read/write access to the Logs database for making log entries, b) provides read/write access to the Consumer Information database for deletion of private information, c) provides read/write access to the Provider Information database for storage, retrieval, and update of provider data (items a-d inclusive as given in the CSAPP.7 bullet of Section 2); in addition, handles write protection for the Provider Information database, and read/write protection for the Logs database (see Section 3.1) to meet the requirements expressed in CSAPP.7.
- *Import P-agent:* receives private information disclosures and updates from other PPCSs; called a P-agent because it is acting for its own PPCS which is acting like a provider PPCS (receives information for processing).
- *Export C-agent:* sends private information disclosures and updates to other PPCSs; sets up secure channels to other PPCSs for sending information disclosures or updates and authenticates the providers at both ends of the secure channel; called a C-agent because it is acting for its own PPCS which is acting like a consumer PPCS (sends out information for processing).

Descriptions of the database and service process components of Figure 1 follow:

- *Provider Information Database:* contains provider information items a-d inclusive as given in the CSAPP.7 bullet of Section 2.
- *Consumer Information Database:* contains consumer information items e) and f) as given in the CSAPP.7 bullet of Section 2; segmented for each consumer.
- *Logs Database:* contains log entries for PPCS-consumer actions such as information collection, information use and disclosure, information access and update, information deletion; segmented for each consumer.
- *Service Processes:* represent the services offered by the provider; the arrow going out of these processes represents a) private information collected by the services, b) provider information (items a-d inclusive as given in the CSAPP.7 bullet of Section 2) for storage or update; the arrow going in to these processes represents private information required to carry out the services.

How can parties who have received private information disclosures be expected to delete the information upon completion of purpose or information expiry? Such parties are considered to be subcontractor providers of the first provider and provide services to the first provider needed to complete the purposes of the first provider. Therefore, the first provider is actually a consumer. As a consumer, the first provider has negotiated a consumer privacy policy with each subcontractor provider, containing the required purposes and information retention times reflecting the wishes of the original consumer. The PPCS of each subcontractor provider then deletes the original consumer's private information upon completion of the purposes in the privacy policy agreed with the first provider or upon information expiry.

Table 1 identifies the PPCS agents that are responsible for meeting each CSAPP requirement (Except for CSAPP.7 which is met by the security measures in Section 3.1).

Table 1. Agents implementing CSAPP requirements

CSAPP Requirement	Agents Responsible
CSAPP.4, Limiting Collection	All agents except import/export agents
CSAPP.5, Limiting Use, Disclosure, and Retention	All agents
CSAPP.6, Accuracy	All agents
CSAPP.8, Openness	Interface C-agent, Controller P-agent, Db access P-agent
CSAPP.9, Individual Access	Interface C-agent, Controller C-agent, Db Access C-agent
CSAPP.10, Challenging Compliance	Interface C-agent, Controller C-agent, Db Access C-agent

3.1. Security

Table 2 identifies security requirements and implementations for the above PPCS agent architecture. Standard protection such as firewalls and intrusion detection systems are assumed in place. Private and sensitive consumer information receives double protection – both encryption/decryption and directory protection. Although we have not specified it in Table 2, some consumers may wish to be anonymous, requiring authentication through blind certificates.

Table 2. Security requirements and implementations for the proposed PPCS agent architecture

Architecture Component or Location	Security Requirement	Security Implementation
PPCS Software Executables	Write Protection	Firewall, Intrusion Detection, Operating System Directory Protection (e.g. Linux)
Database: Provider Information	Write Protection	Operating System Directory Protection (e.g. Linux)
Database: Consumer Information	Read/Write Protection	Operating System Directory Protection (e.g. Linux) plus Public Key Encryption / Decryption (e.g. RSA) in conjunction with SSL
Database: Logs	Read/Write Protection	Operating System Directory Protection (e.g. Linux)
Communication Channel: To Consumer, Consumer Designate, or any Internet User	Secure Channel and 2-way authentication for Consumer or Consumer Designate	SSL for secure channel and authentication of provider; digital certificate to authenticate consumer or consumer designate
Communication Channel: To Other PPCS	Secure Channel and 2-way authentication	SSL for secure channel and authentication of providers at both ends of the channel

3.2. Implementation

Each service provider is expected to offer a PPCS for the service(s) that it provides. The PPCS may be one that is implemented on the provider's premises for its sole use or one that is provided by a PPCS service provider (e.g. privacy protection authority) for use by multiple providers, whose services may be individually too lightweight (either in size or number of customers) to justify the cost of maintaining a PPCS. Provision of the PPCS by a service provider that is a trusted privacy protection authority is a promising approach, since it would undoubtedly result in a higher level of consumer confidence.

Providers will want to install PPCSs to improve business since consumers want assurance of privacy policy compliance. Consumers will choose to do business only with providers that have installed PPCSs. Such providers would have a higher reputation and attract more customers. Providers that don't have PPCSs will realize that it's a cost of doing business and install them.

Critical PPCS components can be made tamperproof by incorporating them in hardware. This can make it very difficult to have illegal access to the consumer's private information and help to avoid unauthorized copying of private information or faking of log entries.

To prevent illegal copying or use of consumer data through malicious service processes that masquerade as legitimate processes, the service processes can be certified by a trusted certification authority and cryptographically keyed with consumer data so that the data can only be used with the certified processes. This keying is a topic for future research.

To promote consumer trust in PPCSs, the latter can be standardized and certified by a trusted certification authority or trusted privacy protection authority (e.g. privacy commissioner belonging to a province or state).

Regarding consumers manually checking the logs for compliance, we note that the Controller C-agent has access to both the consumer's privacy policy and the logs. This agent can be coupled with a graphical display module that would interpret the logs and show graphically which private data was collected and how the data was used. This would make it easier for a consumer to check the logs herself. A consumer would probably have higher confidence in the PPCS if she verified the logs herself since direct evidence carries more weight than relying on another party. If a consumer prefers not to check the logs herself (e.g. computer-shy or lack know-how), one alternative is to have her use a log verification service that can be offered by an Internet firm such as a trusted certificate authority. Another alternative is to have the PPCS implement automatic log verification using the Controller C-agent. This verification process can again be certified by a trusted privacy authority to engender consumer trust in the system.

3.3. Strengths and weaknesses

Some strengths of the proposed agent architecture are:

- Simple agent-based architecture, with clear division of tasks between consumer agents and provider agents will allow for easy implementation and maintenance.
- The provider's explanations of what information it requires for specific purposes as well as how the information will be used and disclosed is open to scrutiny by the entire Internet community, helping to assure the provider's honesty.
- Private information deletion by parties receiving disclosures is handled simply and elegantly through recursion.
- The consumer can verify privacy policy compliance for herself (if desired) instead of having to rely on a third party.

Some weaknesses of the proposed agent architecture are:

- Scalability. Private information disclosures could conceivably spread from the originating PPCS to multiple PPCSs such that the information paths form larger and larger trees. The communications needed to keep disclosed private information and associated privacy policies up-to-date may have a scalability problem as the number of PPCSs increase.
- Security. The consumer's private information can be abused at basically two places: the service processes and databases internal to the PPCS. Although we have suggested remedies in Section 3.2, the remedies are not foolproof. In many cases, we can only provide deterrence by making it as difficult as possible for the attacker to succeed.

3.4. Related work

A closely related work is [7] where the authors described similarities between a system for digital rights management and a system for privacy rights management. The authors examine the feasibility of turning a digital rights system into a privacy rights system. Their approach is centralized whereas we describe a decentralized approach, with the functions of a Data Controller embodied in the PPCS. The authors of [7] also describe extensions to XrML [8] to provide privacy functions. The PPCS would be driven by an XML framework, describing the privacy rules it would follow. This would allow the use of privacy mark-up languages such as APPEL [9] and EPAL [10]. In addition, there are works on security policy compliance or general e-contract enforcement. These works (e.g. [11, 12, 13]) differ mainly from ours in that they deal with the enforcement of complex security policies or business contracts that require automatic program verification of rules expressed in a suitable language; we deal with simpler personal privacy policies with enforcement via secure logs and legal recourse.

4. Conclusions and future work

We have proposed a PPCS agent architecture that largely satisfies the requirements dictated by representative privacy legislation and discussed its strengths and weaknesses. PPCSs are essential for giving consumers confidence that their privacy policies are respected. We have not addressed the following challenges: a) protection from denial of service attacks, b) foolproof protection (e.g. cryptographically keying data to service processes) from illicit use of private information, and c) foolproof techniques for protecting the software executables. We plan to address these in future work as well as prototype the architecture to explore any potential usability or performance issues (e.g. scalability).

5. References

[1] G. Yee, L. Korba, "Semi-Automated Derivation of Personal Privacy Policies", Proceedings, 15th IRMA International Conference, New Orleans, Louisiana, May 23-26, 2004.

[2] G. Yee, L. Korba, "Bilateral E-services Negotiation Under Uncertainty", Proceedings, The 2003 International Symposium on Applications and the Internet (SAINT2003), Orlando, Florida, Jan. 27-31, 2003.

[3] G. Yee, L. Korba, "The Negotiation of Privacy Policies in Distance Education", Proceedings, 14th IRMA International Conference, Philadelphia, Pennsylvania, May 18-21, 2003.

[4] G. Yee, L. Korba, "Privacy Policy Compliance for Web Services", Proceedings, 2004 IEEE International Conference on Web Services (ICWS 2004), San Diego, California, July 6-9, 2004.

[5] Department of Justice, Privacy Provisions Highlights, http://canada.justice.gc.ca/en/news/nr/1998/attback2.html

[6] Canadian Standards Association, "Model Code for the Protection of Personal Information", retrieved Sept. 5, 2003:http://www.csa.ca/standards/privacy/code/Default.asp?articleID=5286&language=English

[7] S. Kenny and L. Korba, "Adapting Digital Rights Management to Privacy Rights Management", Computers & Security, Vol. 21, No. 7, November 2002, 648-664.

[8] Extensible rights Markup Language, retrieved Oct. 8, 2004: http://www.oasis-open.org/cover/XrMLSpec13-200103.pdf

[9] W3C, "A P3P Preference Exchange Language 1.0 (APPEL 1.0)", retrieved April 22, 2004 at: http://www.w3.org/TR/P3P-preferences/

[10] Enterprise Privacy Architecture Language (EPAL), http://www.zurich.ibm.com/security/enterprise-privacy/epal/

[11] D.K.W. Chiu et al, "A Three-Layer Architecture for E-Contract Enforcement in an E-Service Envronment", Proceedings of the 36th Hawaii International Conference on System Science (HICSS'03), 2002.

[12] X. Ao et al, "A Hierarchical Policy Specification Language, and Enforcement Mechanism, for Governing Digital Enterprises", Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks (POLICY'02), 2002.

[13] P. McDaniel and A. Prakash, "A Flexible Architecture for Security Policy Enforcement", Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03), 2003.

[1] NRC Paper Number: NRC 47431