Chapter 7

Security and Privacy Challenges of a Digital Government

James B. D. Joshi, Arif Ghafoor, Walid G. Aref, Eugene H. Spafford
Purdue Universit, West Lafayette, Indiana USA

Abstract: A digital government can be viewed as an amalgam of heterogeneous information systems that exchange high-volume information among government agencies and public and private sectors engaged in government business. This gives rise to several daunting multidomain security challenges as well as concern for citizen privacy. The success of a digital government infrastructure depends on how well it meets these challenges and its preparedness against numerous potential threats ranging from simple act of hacking to cyber-terrorism. In this paper, we outline these crucial security and privacy issues and present various solutions that are available and need to be further investigated.

Key words: security, access control, privacy, multidomain environment

1. INTRODUCTION

A digital government (DG) can be viewed as an amalgam of interconnected heterogeneous information systems in which government agencies and public and private sectors exchange a high volume of information. Several US government agencies have aggressively adopted information technologies in order to modernize the government's highly fragmented service-centric information infrastructure by improving information flow and the decision-making process. Efficient, flexible, interoperable, and securely integrated information systems are needed to achieve such seamless information flow and service integration. Creating such systems requires a holistic development approach to building a secure information infrastructure. Such infrastructure supports both the intricate interdependence of government programs at different levels and between

government and the private and public sectors that have become essential partners in supporting government's public services.

Although Information Age technologies provide intriguing opportunities for developing DG concepts, they also create significant infrastructure security and privacy challenges. The overall grade of "*D*-" for computer security at the Federal Departments and agencies, as per the report published on September 11, 2000, by the Subcommittee on Government Management, Information and Technology, indicates the uphill path the government agencies need to take in order to transform their processes and integrate them within a secure DG infrastructure.

Various goals of information system security include confidentiality or secrecy, integrity, availability, accountability, and information assurance [13]. Three key mechanisms that provide the foundation for an information security include *authentication*, *access control*, and *audit*. Authentication establishes the identity of an entity and is a prerequisite for access control. Access control limits the actions or operations that a legitimate entity performs. The audit process collects data about the system's activity. Once a user is authenticated, the system should enforce access control using an established technique such as a reference monitor that mediates each access by a user to an object.

Several access-control models have been proposed to address the security needs of information systems. Traditional access control approaches fall into two broad categories: discretionary (DAC) and mandatory (MAC). DAC approach lets users grant their privileges to other users, whereas MAC approach uses a classification scheme for subjects and objects. User classification leads to several clearance levels for access control, whereas classification of objects can be established according to their sensitivity. To avoid the unauthorized flow of sensitive information, the MAC model - also referred to as the multilevel model - can enforce no read-up and no write-down rules at a given level [13].

Several security technologies that are becoming indispensable for large distributed and networked heterogeneous systems, like a DG, include *firewalls*, *intrusion detection systems*, *encryption techniques*, *PKI (Public Key Infrastructure) technologies*, etc. Growing privacy concerns over the Internet foreshadows the critical citizen privacy issue in a DG environment because of the huge amount of citizen information it will have in its databases. For a DG infrastructure, designing and implementing these mechanisms and technologies in an integrated manner poses a daunting challenge. We perceive the following three key concerns for a DG infrastructure:

– Secure integration of information systems belonging to government and non-government organizations,

– Citizen privacy that is key to the success of democratic process,
– Threats to the DG infrastructure that can endanger the national security, and their assessment in order to build efficient counter measures.

2. SECURE INTEGRATION OF SYSTEMS

Inherently multidisciplinary and dynamic, a DG's organizational and operational base is characterized by the coexistence of diverse information security policies employed by individual government agencies. These varied policies create a highly heterogeneous multidomain environment. Such environments should support interoperability of several security domains and allow strong inter-domain interaction. Diversity in a multidomain environment may exist in different forms [10]. For example, the environment may be composed of diverse interacting and collaborating constituent agencies with different policies. Similarly, the environment may have more than one security goals or the variations of the same goal. Furthermore, the environment may have heterogeneous system components such as operating systems, databases, etc., each with different security mechanisms [10].

The overall infrastructure must allow seamless and secure interoperation among diverse and heterogeneous security mechanisms. The infrastructure should be scalable, open and extensible. Meeting all these requirements presents several daunting challenges, the key among which include: *semantic heterogeneity*, *secure interoperation*, *risk propagation and assurance*, and *security management*.

2.1 Semantic heterogeneity

The diversity of organizational and user-specific security policies in a DG environment requires powerful formalisms for efficiently mapping security attributes across interacting domains. In a DG environment, coexistence of different security policies or the variations of a single policy can give rise to naming conflicts among similar security attributes, and structural conflicts among user/role hierarchies and access rules. These conflicts need to be resolved by employing an appropriate metapolicy [10]. Such metapolicy models should be generic and flexible enough to express a wide range of security policies and must provide a semantic basis for policy composition and modifications. Metapolicies must also allow autonomy and transparency for the policies adopted by an individual domain, which provides for the policies' continuous evolution.

2.2 Secure interoperability

Any policy change, addition, or deletion requires reevaluating the system's secure interoperability. Secure interoperability poses a major challenge when dealing with an environment where subjects from a different domain access objects in a given domain. The goal is to ensure that no security violations occur during inter-domain accesses. In particular, secure interoperation should enforce the following two principles [7]:

– The autonomy principle, which states that if access is permitted within an individual system, it must also be permitted under secure interoperation.
– The security principle, which states that if an access is not permitted within an individual system, it must not be permitted under secure interoperation.

For example, consider two systems S1 and S2, and assume that user A can access whatever user B can access in S1, and user C can access whatever user D can access in S2. Now, suppose we allow S1 and S2 to interoperate by allowing D to access A's files and B to access C's files. This results in the violation of the security principle, as B can now access A's files through transitivity (B can access C's and hence D's, and consequently A's files), which was not permitted within S1 alone. Hence, the added interoperation links between S1 and S2 result in an insecure multidomain environment.

As indicated by the undecidability result of the safety problem related to secure interoperation [7], in general, it is impossible to guarantee secure interoperation among multiple domains. Furthermore, even the problem of finding a secure solution with some optimality is NP-complete [7]. Optimization can include maximizing the amount of shared data among all domains, maximizing the number of legal accesses, or minimizing the number of conflicting domains.

2.3 Assurance and risk propagation

In a multidomain environment, users must maintain a certain degree of assurance about the entire system's security. While some risks may be acceptable in a local system, such risks can, in a larger network, propagate and increase the level of vulnerability of all interconnected systems. For example, an information system, say S, may be securely interoperating with many other systems, all of which interoperate with each other through system S. In such a case, a security breach in S renders all the interconnected systems vulnerable to attack.

A related issue, the cascading problem, also arises in multidomain environments. Consider two multi-level systems, X and Y. Suppose system X is designed for managing information classified as either *secret* or *top*

secret and that all users of X are cleared for *secret* information at least. System Y can handle information classified as *confidential* or *secret*, and its users are cleared for *confidential* information at least. Now, suppose their owners integrate the two systems, and the resulting three levels of clearance include *confidential*, *secret*, and *top secret*. In the merged system, the *secret* information can pass between the two systems. If a penetrator overcomes the protection mechanisms in both the individual systems, then he can downgrade the *top secret* information of system X to the level of *secret* and pass it to system Y. In system Y, the same penetrator can then downgrade that information to *confidential*. Thus, users having the lowest clearance in either system can access the *top secret* information. This shows that in a DG environment each system should maintain high assurance and be aware of the security assurances of the other systems.

2.4 Management challenges

Security management in a DG infrastructure presents a challenging task because of the large number of administrative domains, subjects, and objects. One characteristic of a DG is that it essentially forms an open system where the entities that represent users, objects, policies, security domains, and other components are transient. This inherent dynamism makes the task of overall management and, in particular, security configuration management, and the management of metapolicies and policy evolution very difficult. Practical and efficient methodologies for security management will be crucial for the success of a DG.

3. APPROACHES TO SECURE INTEGRATION

Several approaches to information security exist that aim to meet the challenges we have described. Here, we profile the strengths and limitations of the most prominent methods, which Table 2 summarizes.

3.1 Policy-metapolicy specification

In a multidomain environment, establishing semantically correct relationships among security policies is essential to ensuring secure cooperation. Metapolicies can specify such relationships as cooperation rules and guidelines for conflict resolution and interaction.

Hosmer [10] proposes several conflict-resolution methods, including manual, standard form, and rule-based strategy approaches. The manual approach, used most commonly, assigns a security officer the responsibility

for manually integrating multiple policies and resolving conflicts. In the standard-form approach, the organization adopts some generic or policy-neutral guidelines to ensure secure interoperability. Each domain uses a conversion logic to translate its local rules to a global metapolicy schema. In a rule-based strategy, the conflict resolution mechanism uses a predefined set of rules such as voting or informal guidelines. For policy mediation, Kuhnhauser's framework uses conflict and cooperation matrices [14]. A conflict matrix provides a ranking mechanism to resolve conflicts between two policies. The cooperation matrix stores the information about a predetermined policy to be used when two domains interact.

Traditional DAC and MAC models lack capabilities for expressing a domain's arbitrary security requirements. Increasingly, flexible approaches are being sought that allow user-defined security policies. One such model is the newly emerging *role-based access control* (RBAC) model that has generated great interest in the security community. Recently, Sandhu and colleagues have proposed the National Institute for Science and Technology RBAC as a standard reference model [17]. RBAC's policy neutrality, constraints, and role hierarchies make it a powerful model for specifying policies from other models such as DAC and MAC and for specifying arbitrary user-specific access rules [17, 19].

RBAC’s flexibility and similarity with organizational concepts make it a good candidate for addressing access control issues in a multidomain environment [15]. Further, models for administrative roles provide efficient mechanisms for distributing security management functions to a number of administrators [19]. Other new access control models that have shown potential for supporting a multipolicy environment include *type enforcement*, *multiple-policy schematic protection* (MSP), *typed access matrices* (TAM), and *dynamically typed access control* (DTAC) models, which use subject and object types [13]. However, these models have reached only the initial phases of their development.

Applications and services in a DG environment require automated transactional functions and workflow-based processing. To support access control in such tansaction-intesive environments, Thomas and colleagues [21] propose an initial *task-based access control (TBAC) family of models in which the authorization unit is a task. However,* much needs to be done for making TBAC useful for real world applications. A viable access control solution proposed by Bertino and colleagues for workflow-based systems is to assign roles to workflow tasks [3].

Public-key infrastructure technology is maturing, and the use of PKI certificates is expected to be ubiquitous in the near future. Certificates issued by a PKI facility can be used for facilitating access control in the networked DG environment. For example, an extended X.509 certificate, issued by a

certification authority, can carry user information [17]. These techniques can be used to either support a host's access control method by carrying access control information or provide a separate access control mechanism based on trust centres. Table 1 summarizes various access control approaches discussed and their important features.

Table 1. Access control approaches and features compared

Approach	Features
DAC	Ownership based, flexible, most widely used, does not provide high degree of security, and hence low assurance
	Typed versions such as SPM, TAM and DTAC are expressive but have little or no experience base
	DTAC can handle dynamic changes and task based control
	Most cannot be used where classification levels are needed
	Typed versions have tried to include classification levels
MAC	Administration based,
	Information flow control rules; uses classification labels
	High level of security, and hence high assurance, but less flexible.
RBAC	Policy-neutral/flexible; Principle of least privilege
	Separation of duty; Easy administrative features
	Able to express DAC, MAC and user-specific
	Can be easily incorporated into current technologies
	Good potential for use in multidomain environments when policies are expressed using role hierarchies and constraints
Access control tasks/workflow systems	Task-oriented authorization paradigm, RBAC for WFMS
	TBAC is at an initial stage of development
	Key for success of transaction intensive DG environment
Certificate-based	Utilization of existing PKI facilities
	Complements the host’s access control model
	Can use trust centers in the WWW

3.2 Architectural methods

Approaches that address the challenges of large multidomain environments also address architectural issues. Notable among these are the Object Management Group's Common Object Request Broker Architecture (CORBA) and the Open Software Foundation's Distributed Computing Environment. CORBA offers a security policy specification but lacks formal semantics, thus making security-handling mechanisms more or less ad hoc. DCE addresses the general issue of object interoperability by providing a middleware architecture that implements an ad hoc security mechanism.

Some other proposed architecture includes the Distributed Trusted Operating System (DTOS) and the Meta Object Operating System Environment (MOOSE) [8]. DTOS supports separation between the policy

specification and policy enforcement components by using a mix of tabular representation and a language-based specification model to provide a high degree of flexibility in security policy selection. MOOSE's three-layer architecture uses a formal approach to integrate modelling, specification, verification, and implementation [8].

Software agent based architectures are emerging as possible solutions for addressing the DG's multidomain security issues. Agents are characterized by *adaptation*, *cooperation*, *autonomy*, and *mobility*. Agent communication languages, with extensions, can be used to negotiate policies during conflicts to ensure secure interoperation [HE8]. The servers and clients in a distributed environment can assign policy negotiation and security enforcement tasks to agents. Although the mobility and adaptability characteristics of agents provide essential features for the efficient use of system resources, they themselves can pose several security threats. For example, an agent can engage in malicious behaviour, thus disrupting the host's normal operation. Similarly, a host can hinder an agent's activity by denying required access to local information resources.

Table 2. Digital government security challenges and potential approaches to solving them

Challenges	**Solution approaches**
Semantic Heterogeneity	Generic language (such as Z), algebraic, security automata
	Policy neutral models such as RBAC
	Typed extensions of access control matrix models such as TAM and DTAC
	Programmable security; Export security interfaces
Secure interoperation	*Conflict types*
	Domain conflict, Rule conflict
	Conflict resolution approaches
	Manual, need-based, priority based, voting etc.
	Composition operators such as Union, Intersection, Product
	Hierarchy of security properties; Virtual roles/Role mapping in RBAC
Flexibility/ Extensibility	Separation of policy specification and enforcement components
	Policy library/Policy habitat, Layered architecture
Risk control/ Assurance	Safety analysis such as static and dynamic checking in DTAC
	Use of least privilege feature in RBAC system; Inline coding
	Retain reference monitor properties of tamperproof, complete mediation and verifiability
Management	Administrative models such as administrative role based models
	Auditing; Risk, vulnerability analysis
	Security assessment and certification, Layered architecture

3.3 Database federation approach

The database federation approach, which integrates several database management systems, provides some solutions to the multidomain problem and is relatively a mature field. Several researchers have proposed approaches for developing systems that achieve the autonomy of component databases yet remain transparent at the federation level. These approaches also address a multidomain environment's security management issues. For example, Jonscher and Dittrich's federated database system allows DAC and MAC policies within component databases [12]. This system uses a global access layer to map global authorizations into the local-access rights of individual databases. The Distributed Object Kernel [20] is another example of a secure federated database system that uses a mapping technique to build a global-access policy from local DAC and MAC policies. In the DOK system, the enforcement mechanism for global security involves layered processing by agents designed to check attribute constraints and sanitize query results. Approaches for federated-database schema integration can be extended for developing metapolicy frameworks for access control in a multidomain environment and to provide a viable security management solution for a DG infrastructure.

4. CITIZEN PRIVACY

A fairly common definition of privacy is "*the right of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated*" [11]. As shown by various surveys [1], personal privacy in the Internet is a big concern for users, and it has been so for many years. The recent move towards the development and deployment of a new digital Interactive TV technology that have the capability to track each TV show a viewer watches and profile the viewing as well as spending habits of people, adds a new dimension to the already growing privacy concerns over the Internet [22]. The DG infrastructure that essentially builds on these Internet technologies thus carries over a new level of concerns for citizen privacy.

In a DG environment, user transactions for the government services will essentially use various sensitive personal information such as social security numbers, tax information, criminal records, medical information, etc. Besides, a DG environment allows increased connectivity of businesses to government information systems. This calls for extra measure on the part of the DG infrastructure to provide protection of personal information in huge government databases and sensitive information in transit. Compromising a

single DG component can leak out huge amounts of personal information in its databases to the non-government systems connected to it. Access to social security numbers by identity thieves provides them with a much more power to abuse in a DG environment as this allows them to potentially access any information about a person stored in government databases. Billions of records are estimated to be available in both private and government databases that describe each citizen's finances, interests, and demographics. Privacy vulnerabilities arise even if data is available in statistical or aggregate forms that allow personal information to be inferred [11]. Furthermore, the fact that the government carefully monitors every transaction and resource access made by a citizen can discourage citizen participation.

End users are exposed to several security and privacy risks when using Web browsers, which will play an essential part as DG interfaces. Browser vulnerabilities can be used to compromise client security and user privacy [6, 16, 13]. Cookies, the data stored on the client's machine and exchanged between the clients and the server to maintain connection information, can be used for the purpose of gathering user information. Use of executable contents, such as Java applets, ActiveX controls, etc. is another source of security vulnerability [13]. Firewall technology has become the most popular defense for network servers against the open untrusted Internet. Though firewalls can prevent illegitimate traffic from travelling from the global Internet to DG networks, legitimate requests that pass through a firewall may be used for a data-driven attack on the networks or back-end systems [6, 16]. Configuration of firewalls and network servers is a formidable and error prone task.

5. APPROACHES TO CITIZEN PRIVACY

In a DG environment, a conflicting situation is that while enhanced capability of carefully monitoring user activity is desirable to detect malicious activities against the DG infrastructure and to achieve accountability, it conflicts with the privacy concerns of citizens. The success of a DG environment will depend on how well it balances its ability to monitor malicious activities and its ability to establish itself as a fully trustworthy and secure medium. An effective solution for privacy in such an open DG environment will require a combined effort from technological, legislature and public policy sectors [11]. Encryption and PKI technologies provide reasonable solutions to the *communication privacy* that concerns with the privacy of the information in transit [11]. However, adequate

technical measures do not exist that address the authorized use of sensitive personal information in databases (*database privacy*).

A forthcoming proposal is to develop new access control models or extend existing ones that are capable of addressing privacy constraints as access rules. As pointed out by Samarati [11], such an access authorization model should include: explicit permissions provided by owner, permission based on the use and purpose of information, permissions to control dissemination, permissions based on time and external conditions, etc. Such privacy-oriented mechanisms are lacking and this can become a deterrent to the success of the DG. Several tools such as web anonymizers, remailers, encrypted authentication, currently provide support for achieving some level of privacy. However, there also are tools that offset these, such as snoopware that locate personal data on the web, stealthware that essentially monitors client behaviour, etc.

6. THREATS TO THE DG INFRASTURCURE

As Internet acts as the global platform that provides universal access to a DG infrastructure, all kinds of cyber attacks can be targeted towards the DG environment. Furthermore, as a DG environment is a monolithic multidomain system of securely interconnected heterogeneous systems, such attacks can have highly exacerbated effects. For example, a simple denial of service attack at some key government systems may have a very damaging effect on the services provided by other interconnected systems, rendering essential government services inoperative. Even bigger concern is the protection of critical infrastructure components within the DG. Thus, higher level of security assurance will be desirable for each individual domain. Further, independent as well as collaborative techniques must be developed to counter such threats. It is expected that in few years the cyber-threats to the country is expected to be worse than the physical threat [2]. At the worst, a DG infrastructure can be considered as a system with a single point of failure.

Potential "*info weapons*" that can be used to launch attack on a DG government, as are done over the Internet, include computer viruses, logic bombs, worms, Trojan horses, etc [2, 5, 6]. Various attacks on systems include denial of service attack, virtual sit-ins and blockades, rootkits, etc [5]. The attacks using these malicious tools range from simple hacktivism to the more damaging cyber-terrorism and info-war [5]. Cyber-terrorists can target civilian infrastrucure, military infrastructures or economic sector, or all at once to launch a complete infowar against the country.

Within the Internet, hacktivism refers to active hacking activities with the intent to disrupt normal operations but not causing serious damage [5], whereas cyber-terrorism refers to the use of act of terror over the cyberspace. Aimed against the DG infrastructure, a simple hacking can have grave consequences. For example, an hour-long properly coordinated hacking activity that affects the country's air traffic system, a critical infrastructure, can have very drastic consequences. Several instances of hacktivism in last few years have been discussed in [2, 5].

A recent survey conducted by Computer Security Institute (CSI) and FBI, reports that 71% of enterprises surveyed had detected unauthorized use by insiders in 2000 [16]. Similar results have been reported by the security survey conducted by Information Security Magazine (ISM) [4]. This indicates that the insider threat is real and can have more damaging effect than the external threat. In a DG environment, such security breaches through disgruntled insiders can put the whole nation at risk. As Shaw and colleagues point out, "*staff employees pose perhaps the greatest risk in terms of access and potential damage*" to the DG environment, particularly, "*the part that constitutes the critical infrastructure of the country*" [18].

Table 3. Threats and their intent [2]

Threat level	**Actor**	**Intent**
National security threats	Information Warrior (Cyber-soldier)	Reduce decision making capability at the national level, National chaos and psychological terror
	National intelligence (Cyber-spy)	Information leakage for political, military and economic advantages
Shared threats (government & private sector)	Cyber-terrorist	Visibility/publicity, chaos, political changes
	Industrial espionage	Competitive advantage
	Organized crime (Cyber-crime)	Revenge, retribution, monetary gain, institutional/political change
Local Threats (Hacktivism)	Institutional hackers	Monetary gain, thrill/challenge, publicity/prestige
	Recreational hacker	Thrill, challenge

Table 3 shows various threat levels and the criminal intent behind them [2]. At the highest level, we see national security threats, which are essentially aimed at the nation's critical infrastructure. Threats common to both government and non-government agencies include cyber-terrorism and e-espionage. Finally, there are frequently occurring hacking incidents that can create huge losses within a DG environment. So far, there is no nationally coordinated defense capability to detect and counter strategic and well-coordinated act of cyber-terrorism against the nation [2, 5].

7. APPROACHES AGAINST THREATS TO DG

As indicated by the ISM survey [4], a key technical problem related to the insider attack is the inadequate policy specification and enforcement. Proper management of authorization policies, and policies as to the use of various software programs such as e-mails, browsers, etc. and use of up-to-date virus protections can greatly reduce insider attacks that can often be considered accidental or unintentional. Such unintentional insider security breaches can largely be avoided through education and awareness. Approaches using separation of duty and granting of least privilege to users can greatly reduce the misuse of resources by an insider. In such cases, use of formal models such as RBAC and DTAC can drastically improve the management complexity. The gravity of insider threat in a DG environment accentuates the need for proper monitoring of not just the technical activities of employees with crucial knowledge of the working of the DG infrastructure, but also their personal traits to detect any deviant behaviour. Doing that requires a careful balancing act between monitoring employee activities and maintaining citizen privacy.

A balanced and integrated use of various security technologies will be essential to secure the overall DG infrastructure from external threats. Intelligent distributed capabilities will be required to detect and counter both structured and unstructured attacks against the DG infrastructure. A difficulty, as pointed out by Denning, is the proper assessment of cyber-threats that can have national risk [5], particularly because such incidents have not been encountered.

8. CONCLUSION

Several daunting challenges exist towards the development of a secure DG infrastructure. As it facilitates the functioning of the entire country, ensuring its security is of utmost importance.

Foremost is the problem of secure integration of information systems of various government and non-government agencies in order to streamline government services. Of the many access control approaches, RBAC models appear to be the most attractive solution for securing the multidomain DG environment. In essence, RBAC models can provide a generic framework for expressing diverse security requirements. Integration of such access control models with encryption and PKI technologies can provide pragmatic solutions to the complex DG infrastructure.

Federated database management system approaches show promise and will likely be expanded to effectively address general multidomain issues.

Agent systems, on the other hand, require further exploration to evaluate their security enforcement features. Developing efficient techniques to evaluate security assurance and carry out risk analysis remains a major challenge.

Threat assessment and the development of coordinated, distributed capability to detect and counter them will be very crucial for the success of the DG. There is a critical need for developing privacy models and mechanisms. Furthermore, it is essential to pursue multidimentional approach to citizen privacy that combines well-coordinated technical, legal as well as organizational and public efforts.

Acknowledgement: The research presented in this paper has been funded by a grant from CERIAS.

References

[1] M. S. Ackerman, L. F. Cranor, J. Reagle, "Privacy in e-commerce: examining user scenarios and privacy preferences"; *Proceedings of the first ACM conference on Electronic commerce*, 1999, Pages 1 – 8.

[2] Y. Alexander, M. S. Swetnam, *Cyber Terrorism and Information Warfare I, Assessment of Challenges*, Oceana Publisher Inc./Dobbs Ferry, New York,1999.

[3] E. Bertino, E. Ferrari, V. Atluri, "The Specification and Enforcement of Authorization Constraints in Workflow Management Systems," *ACM Transactions on Information and System Security*, Vol. 2, No. 1, Feb. 1999, pp. 65-104.

[4] A. Briney, "Security Focussed", *Information Security Magazine*, September, 2000, Pages 40-68.

[5] D. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", *Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop*, December, 2001.

[6] S. Garfinkel, E. H. Spafford, "Web Security & Commerce," *O'Reilly & Associates*, Inc., Sebastapol, CA, 1997.

[7] L. Gong and X. Qian, "Computational Issues in Secure Interoperation", *IEEE Transaction on Software and Engineering*, Vol. 22, No. 1, January 1996.

[8] J. Hale, m. Papa, S. Shenoi, "Programmable Security for Object-Oriented Systems"", Proceedings", *Database Security XII: Status and Prospects*, S. Jajodia (eds), Kluwer Academic Publishers, 1998, pp. 109-123.

[9] Q. He, K. Sycara, Z. Su, "A Solution to Open Standard of PKI", *Proceedings of the Third Australian Conference*, Eds. - Colin Boyd, Ed Dawson, ACISP'98, Brisbase, Australia, July 13-15, 1998.

[10] H. H. Hosmer, "Metapolicies I", *ACM SIGSAC Data Management Workshop*, San Antonio, TX, December, 1991.

[11] "Database Security XII Status and Prospects", Editor: Sushil Jajodia, *IFIP TC11 WG11.3 Twelfth International Working Conference on Database Security*, July 15-17, 1998, Chalkidiki, Greece.

[12] D. Jonscher, K.R. Dittrich, "Argos – A Configurable Access Control System for Interoperable Environments" *Proc. of the IFIP WG 11.3 Ninth Annual Working Conference on Database Security*, Rensselaerville, NY, August 1995.

[13] J. B. D. Joshi, W. G. Aref, A. Ghafoor, E. H. Spafford, "*Security models for web-based applications*", *Communications of the ACM* , 44, 2 (Feb. 2001), pages 38-72.

[14] W. E. Kuhnhauser, M. K. Ostrowski, "A Formal Framework to Support Multiple Security Policies", *Proceedings of the 7th Canadian Computer Security Symposium*, Ottawa, Canada, May 1995.

[15] S. Osborn, "Database Security Integration using Role-Based Access Control", *IFIP WG11.3 Working Conference on Database Security*, Aug. 2000.

[16] R. Power, ""Tangled Web": Tales of Digital Crime from the Shadows of Cyberspace," *Que/Macmillan Publishing*, Aug. 31, 2000.

[17] *Proceedings of The Fifth ACM Workshop on Role-based Access Control*, Berlin, Germany, July 26-27, 2000

[18] E. D. Shaw, K. G. Ruby, J. M. Post, "The Insider Threat to Information Systems", *Security Awareness Bulletin* No. 2-98, published by Department of Defense Security Institute, September 1998.

[19] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman, "Role-Based Access Control: A Multi-Dimensional View", *Proceedings of the 10th Annual Computer Security Applications Conference*, Orlando, FL, December, 5-9, 1994, pages 54-62.

[20] Z. Tari, G. Fernandez, "Security Enforcement in the DOK Federated Database System", *Database Security X: Status and Prospects*, P. Samarati, R. Sandhu (eds), Chapman & Hall, 1997, pp. 23-42.

[21] R. K. Thomas, R.S. Sandhu, "Task-based Authorization Controls (TBAC): A family of Models for Active and Enterprise-oriented Authorization management", *Proccedings of the IFIP WG11.3 Workshop on Database Security*, Lake Tahoe, California, August 11-13, 1997.

[22] “TV That Watches You: The Prying Eyes of Interactive Television”, A report by *Center For Digital Democracy*, http://www.democraticmedia.org/privacyreport.pdf, June, 2001.