By Rafae Bhatti, Elisa Bertino, *and* Arif Ghafoor

An Integrated Approach to Federated Identity and Privilege Management in Open Systems

Online partnerships depend on federations of not only user identities but also of user entitlements across organizational boundaries.

Web-based collaboration in the highly networked enterprise environment is essential for maintaining strategic online partnerships. The way access to enterprise resources is managed there is critical to ensuring their security. Moreover, the major industrial vendors of security solutions feel that today's collaborative and interconnected e-business landscape requires a secure and effective way for enterprises to share trusted user identities and entitlements.[1] The ability to federate identity across organizations while maintaining access rights and privileges is a major challenge when securing any online business collaboration [5].

Federated identity and privilege management is the key to seamless and

[1] Federated Identity white paper, RSA Security Inc. (https://www.rsasecurity.com/products/FIM/pdf/FID_WP_0405.pdf).

secure enterprise integration and collaboration on the Web. However, almost all well-known schemes for implementing this solution involve necessary tradeoffs specific to an application environment, rendering the solution less useful for broader purposes. Additionally, the development of Web-based federated identity solutions has advanced more rapidly compared to Web-based privilege management mechanisms. The result is a wide gap between the federated identity and privilege management mechanisms and calls for an integrated approach to provide a comprehensive access management solution. Because this disparity is so alarming, the migration of enterprise operations onto the Internet demands a significant evolution of traditional access management mechanisms for securing dynamic Web-based resources [5]. Federated identity and privilege management are both cornerstones of an access management framework and critical to the effectiveness of the overall mechanism.

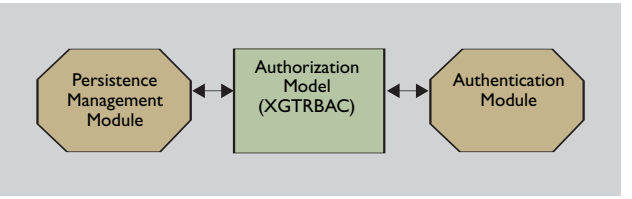

Figure 1. Design methodology for the proposed solution.

Here, we discuss the shortcomings of federated identity mechanisms and their integration with privilege management mechanisms. We also present an integrated approach to federated identity and privilege management specifically designed for Web-based platforms. Any such mechanism should first satisfy several requirements:

Single sign-on (SSO). SSO implies the persistence of user identity and entitlement across multiple enterprise domains. Although many SSO solutions are available, the widening gap between identity federation and privilege management involves many challenges regarding the granting of SSO access to collections of resources and contradictory access-protection rules [5].

Effective access control. An access management solution relies on the access control model and should support a fine-grain, context-aware access control that manages user access to dynamically evolving enterprise resources. Examples of context-aware access control are constraints on resource access based on contextual parameters (such as time and location) when multiple parties with varying time- and location-sensitive access requirements are involved in a partnership. This requirement is particularly challenging in a Web-based environment.

Decentralized model. Decentralization implies that the system does not rely on a centralized or single point for accessing user authentication and authorization information. It is motivated by market demand for B2B scenarios where organizations consider it desirable to have a decentralized model for federating user identities and entitlements, thereby avoiding a scenario where one enterprise essentially authenticates the world population.

Authentication for strangers. Internet service providers cannot assume advance knowledge of the identities or capabilities of all users. The use of an identity- and capability-based credential in most existing systems is a major bottleneck to achieving the objective of authenticating previously unseen users.

Trust, anonymity, privacy. Privacy protection is increasingly important to overall business collaboration, especially from a social and legal perspective. It challenges organizations to deliver sufficient anonymity and privacy without compromising security. The paradox is that while avoiding name-binding appears viable for preserving privacy, name-binding complicates accountability when establishing trust between organizations in online partnerships.

Standardized approach. With so many schemes in various stages of adoption, it is only prudent for organizations to take an incremental, "integrateable" approach, designing new solutions that complement existing standards. We have evaluated the existing technologies, attempting to address only the open issues; for other functionality, we provide hooks within our proposed approach where existing standards can be tied into.

Authorization Protocols

The concept behind federated identity and privilege management mechanisms is motivated by the classical authentication and authorization protocols. A seminal work in authentication protocols [12], implemented as Kerberos (web.mit.edu/kerberos/www/), uses identity-based credentials issued by a centralized server. It, as well as other identity-based schemes, involves scalability problems in distributed systems. Alternatively, a number of schemes have emerged for distributed authorization using capability-based credentials. Notable among them is RFC 2511 [4, 8] based on the public key infrastructure (PKI). The PKI-based approach to distributed access control is traditionally known as trust management (TM); we refer to the credentials used in TM schemes as TM credentials.

In the PKI-based authorization schemes, TM cre-

With so many schemes in various stages of adoption, it is only prudent for organizations to take an incremental, or "integrateable," approach, designing new solutions that complement existing standards.

1. User Bob **needs to access a library resource, say** "CACM_Vol8_No2"**, through his local library login.**
2. The local library (LibBob) **is part of a digital library federation** (FedDigLib)**.**
3. "CACM_Vol8_No2" **is not available locally but at another library** (LibElse) **which is part of** FedDigLib**.**
4. LibElse **categorizes all resources.** "CACM_Vol8_No2" **is categorized as** "LibResourceLevel2"**.**
5. LibElse **is not aware of any user** Bob**, but has a resource access policy that is not based on user identity. Instead, it is based on attributes that a user must satisfy depending on the resource category.**
6. The access policy for category "LibResourceLevel2" **requires a user to provide attributes that include a date of birth (to establish age) and a valid driver's license. It also restricts the resource access to 2 days.**
7. LibElse **publishes the resource metadata that includes the attributes required for access together with a list of attribute authorities** LibElse **trusts. The metadata is available at a well-known URL.**

Figure 2. A Web-SSO request motivating use of property-based credentials.

dentials exhibit properties not suitable for our purposes. The standardized X.509-based TM credential is identity-oriented and tends to have long-lived name binding, making it ill-suited to expressing distributed authorizations. The use of key-centric TM credentials in [4, 6] removes the dependency on names. However, the binding of the access control credential with the key blurs the distinction between authentication and authorization, thereby tightly coupling them. Such an approach limits the expressiveness (and hence effectiveness) of the access control mechanism, since not all system-specific capabilities may be known in advance in a distributed environment and included in a single TM credential. This limitation of the TM credential is a special concern if SSO is to be supported, because SSO is intended to prevent having multiple authorization mechanisms for access to multiple resources.

The next generation of distributed authorization models [1, 3, 7–11] attempts to alleviate that limitation by designing effective and more expressive access control schemes; many such models employ the Role Based Access Control (RBAC), which uses organizational roles (as opposed to identities and capabilities) as a basis for privilege assignment. However, there are shortcomings in these schemes as well.

The X.509-based Privilege Management Infrastructure and its reference implementations (such as PERMIS [7]) employ a name-binding approach. Another emerging specification is the XML-based Access Control Markup Language, or XACML (xml.coverpages.org/xacml.html). Even though XACML doesn't directly support role-based access control, an XACML profile is available for RBAC. The current version (version 02) of this profile of the XACML profile for RBAC doesn't capture all essential RBAC features (such as separation of duties and session-based authorization management). XML-based Generalized Temporal Role Based Access Control (X-GTRBAC) and OASIS [1, 3] are similarly expressive specifications that use RBAC to define dynamic fine-grain access control in an enterprise environment. Meanwhile, all these schemes use either identity-based or capability-based credentials and are not scalable to role assignment for unknown users on the Internet.

Another scheme based on PKI [9] uses the Trust Policy Language (TPL) to map holders of public key certificates to roles. The Role-based Trust management framework [11] merges features from TM and RBAC, using a more expressive policy language compared to TPL. The TM credentials used in [9, 11] are examples of property-based credentials that allow user authentication and subsequent authorization based on certain properties of the user. They are used to authenticate unknown users into known roles, since predefined identities and capabilities are not assumed. However, both schemes have shortcomings with respect to our requirements. For one, they do not support an elaborate access control scheme beyond the basic permission-to-role assignment mechanism in RBAC. Another is that the PKI-based approach in [9] uses X.509-based credentials and hence adopts a name-binding approach.

Finally, none of these schemes satisfies the SSO requirement—a fundamental component of federated identity. Microsoft Passport—the most popular Web-based SSO system today—is based on a centralized server model and is much like a Kerberos counterpart for the Web. However, when dealing with the scale of the Internet, the centralized approach involves peculiar risks, including compromise of the central repository and subjugation to denial-of-service attacks. A centralized model is antithetical to the distributed

nature of the Internet [10]. Two prominent SSO mechanisms—Shibboleth and Liberty Alliance, both offering implementations of identity federation protocols—are based on a decentralized approach. However, they are limited to supporting distributed authentication, not specifying and enforcing access control policies.

Element Type	Element Name	Purpose
RBAC Element	*XML User Sheet (XUS)*	Declares the users and their authorization credentials
	XML Role Sheet (XRS)	Declares the roles, their attributes, role hierarchy, and any separation of duty and temporal constraints associated with roles
	XML Permission Sheet (XPS)	Declares the available permissions
RBAC Assignments	*XML User-to-Role Assignment Sheet (XURAS)*	Defines the rules for assignment of users to roles; these assignments may have associated temporal constraints
	XML Permission-to-Role Assignment Sheet (XPRAS)	Defines the rules for assignment of permissions to roles; these assignments may have associated temporal constraints
RBAC Constraints	*XML Separation Of Duty Definition Sheet (XSoDDef)*	Defines the separation of duty constraints on roles
GTRBAC Constraints	*XML Temporal Constraint Definition Sheet (XTempConstDef)*	Defines the temporal constraints on role enabling and activation; also defines temporal constraints for user-to-role and permission-to-role assignments
	XML Trigger Definition Sheet (XTrigDef)	Defines context-based triggers for invocation of periodic events subject to associated constraint evaluation
Authenticating Credentials	*XML Credential Type Definition Sheet (XCredTypeDef)*	Defines the available credential types

Table 1. Features of X-GTRBAC.

Proposed Solution

We address the problem of how to improve identity and privilege management through an interoperable and modular design of underlying authentication and authorization mechanisms. Our solution integrates a decentralized SSO mechanism within an authorization model by adapting it to use property-based TM credentials and incorporate support for credential management.

A basic requirement our authorization model must satisfy is suitability to Web-based applications. To do so, we chose X-GTRBAC as the access control specification language [3]; it has been shown to be effective in enabling access control in dynamic Web-service applications [3] due to its XML-based modular and flexible context-aware policy specification (see Table 1). The complete grammar specification of X-GTRBAC and a discussion of its use for federated access management is available in [2]. The central idea is that the X-GTRBAC system uses credentials supplied by users to assign them to roles, or authentication, subject to assignment constraints. Users might subsequently access resources according to their role memberships, or authorization, subject to access constraints. Hence, X-GTRBAC supports fine-grain attribute-based access control together with a modular authentication and authorization mechanism. Figure 1 outlines how we adapt the model for Web-based SSO.

We designed the system's interface so it supports, without duplicating, the functionalities available in existing standards. Although many specifications are in the works, the Security Assertion Markup Language, or SAML (xml.coverpages.org/saml.html), is being hailed by the business community as the most promising enabling technology for SSO. SAML, a protocol for message exchange among autonomous business entities, can be used to encode security attributes and decisions, or "assertions." However, SAML is not a self-sufficient mechanism for ensuring SSO, as it lacks authentication and authorization support. It does allow the communicating entities to exchange security information in a decentralized manner but does not establish, check, or revoke any information on its own.

A mechanism is therefore needed for SAML to tie into. Our X-GTRBAC-based specification provides one, designed to accept SAML-encoded assertions as a form of credential. However, this straightforward integration is not sufficient for our purposes—integrating privilege management with existing federated identity mechanisms. SAML assertions are inherently subject to the same name-binding problem that exists in the protocols (such as Kerberos and X.509) it is designed to work with. A recent proposal [6] aimed at integrating SAML with an access-control mechanism suffers from the same drawback. Our specification

Future challenges include integrating our specification with existing directory schemes to support property-based credentials, trust negotiation protocols for incremental attribute collection, and state information for anonymous users to ensure proper accountability.

SAML Credential	X-GTRBAC Instance	Mapping Rules
<Assertion id="LibElseResL2"> <Issuer format="entity"> www.my-attribute-authority.com </Issuer> <AuthnStatement>…</AuthnStatement> <AttributeStatement> <Subject> <NameID format="persistent"> Bob's public key </NameID> </Subject> <Conditions> <NotBefore> 2005:01:30</NotBefore> <NotOnOrAfter> 2006:12:31</NotOnOrAfter> </Conditions> <Attribute name ="DOB"> <AttributeValue> 1978:05:21 </AttributeValue> </Attribute> <Attribute name ="DLN"> <AttributeValue> 0991-09-0991 </AttributeValue> </Attribute> </AttributeStatement> <ds:Signature>…</ds:Signature> </Assertion>	<XUS xus_id="LibElseXUS"> <User user_id ="any"> <UserName/> <CredType cred_type_id = "LEResL2" type_name = "LibElseResL2"> <Header> <Issuer> www.my-attribute-authority.com </Issuer> <Principal mode="persistent"> Bob's public key </Principal> <Validity> <NotBefore> 2005:01:30</NotBefore> <NotOnOrAfter> 2006:12:31</NotOnOrAfter> </Validity> <DSig>…</DSig> </Header> <CredExpr > <Attribute name="DOB"> 1978:05:21</Attribute> <Attribute name="DLN"> 0991-09-0991</Attribute> </CredExpr> </CredType> </User> </XUS>	- User@user_id = **auto generated** ("any" **if** NameID@format="persistent") - NameID->UserName **(empty if** NameID@format = "persistent") - CredType@cred_type_id = **auto generated** -Assertion@id -> CredType@type_name - Issuer -> Issuer - NameID-> Principal - NameID@format -> Principal@mode - NotBefore->NotBefore - NotOnOrAfter->NotOnOrAfter - ds:Signature -> DSig - Attribute@name-> Attribute@name - AttributeValue ->Attribute

Table 2. Credential configuration in SAML profile for X-GTRBAC.

#	Constraint	X-GTRBAC Instance	Meaning
1.	Role Assignment	<XURAS xuras_id="LibElseXURAS"> <URA ura_id="uraBorrowerL2" role_name="BorrowerL2"> <AssignUser user_id="any"> <AssignConstraint> <AssignCondition cred_type= "LibElseResL2" d_expr_id="TwoDays"> <LogicalExpr> <Predicate> <Operator>neq</Operator> <FuncName>hasValue</FuncName> <ParamName>DLN</ParamName> <RetValue>null</RetValue> </Predicate> <Predicate> <Operator>neq</Operator> <FuncName>hasValue</FuncName> <ParamName>DOB</ParamName> <RetValue>null</RetValue> </Predicate> </LogicalExpr> </AssignCondition> </AssignConstraint> </AssignUser> </URA> <XURAS>	The role BorrowerL2 can be assigned only to a user who possesses the credential LibElseResL2 (defined in the XUS document in Table 2). The assignment condition includes rules on credential attributes and asserts the existence of the DLN and DOB attributes. The assignment condition also refers to a duration expression that implements the restriction that the resource can be borrowed for only two days. The duration expression is defined in the XTempConstDef document in our system (see Table 1).
2.	Role Delegation	<XRS xrs_id="xrsBorrowL2"> <Role role_id="rBorrowerL2" role_name="BorrowerL2"> <Junior>BorrowerL1</Junior> <DelegationConstraint> <DelegationCondition d_expr_id="OneWeek"/> </DelegationConstraint> </Role> </XRS>	The role BorrowerL2 can be delegated only if the delegation constraint is satisfied. The delegation condition on the role refers to a duration expression that imposes a restriction on the time period of the delegation. The duration expression is defined in the XTempConstDef document in our system (see Table 1).

Table 3. Constraint specification in X-GTRBAC, representing only a subset of X-GTRBAC access constraints; for the complete specification, see [3].

works with property-based TM credentials, creating a SAML profile for X-GTRBAC involving the feature set from the SAML specification (v2.0). Using a SAML profile in the X-GTRBAC system requires a translation from SAML encoding to the X-GTRBAC format, and vice versa, using Extensible Stylesheet Language Transformations, a standard for syntax-oriented XML document transformation.

Policy Configuration Semantics

To help focus this discussion, we use the Web-based SSO request in Figure 2 as a running example. Table 2 outlines the credential configuration using the SAML profile for X-GTRBAC in the context of this example. It uses features from SAML v2.0, allowing this credential configuration to be adopted by all entities using SAML-compliant protocols. The credential is represented by a SAML assertion. We include only the attributes and elements relevant for this discussion, omitting the namespace prefixes here. Table 2 also includes mapping rules for translating a SAML assertion to the X-GTRBAC format. The X-GTRBAC credential is represented as an XML User Sheet (XUS) document in our system, as in Table 1.

Credential configuration involves several key features:

Property-based credential. Of particular interest for our purposes here is the configuration of TM credentials in property-based mode, making possible authentication for unknown users, since identity is not assumed to be known. If a user name is not provided in the SAML credential, the corresponding credential in X-GTRBAC is constructed by our system using the reserved word "any," representing any anonymous user. When using this reserved word, the credential acts as a nonidentity certificate that does not include the identity of the subject but only a public key (or hash of the key). The nonidentity-based binding is indicated by the value of "persistent" for the format attribute of NameID element in the SAML assertion. Persistent is a format for NameIDs in the SAML standard, allowing opaque values (such as random hashes) to be used in our system in place of subject names to support anonymity and privacy. Note that name-binding credentials can be used if desired, indicated by the appropriate value (such as X.509

Subject Name and Kerberos Principal Name) of the format attribute of NameID element, per the SAML standard (such as X.509 Subject Name and Kerberos Principal Name).

Authenticating attributes. The AuthnStatement element in the SAML assertion contains the authentication context used to generate the authenticator, or credential, for the subject. The attribute information contained in the credential is not necessarily owned by a centralized entity and can be collected from multiple attribute authorities. The authentication statement for a subject can be obtained in practice by invoking the SAML authentication request protocol on an identity provider. The provider responds with the authentication statement and might optionally also include attribute statements. The protocol includes the specification of a metadata repository from which required resource attributes may be learned and obtained using the attribute authorities indicated in the resource metadata. The focus of our approach is not on attribute collection and credential generation. We instead designed the specification to work with SAML assertions that already include credentials generated through prior means (such as using the SAML authentication request protocol).

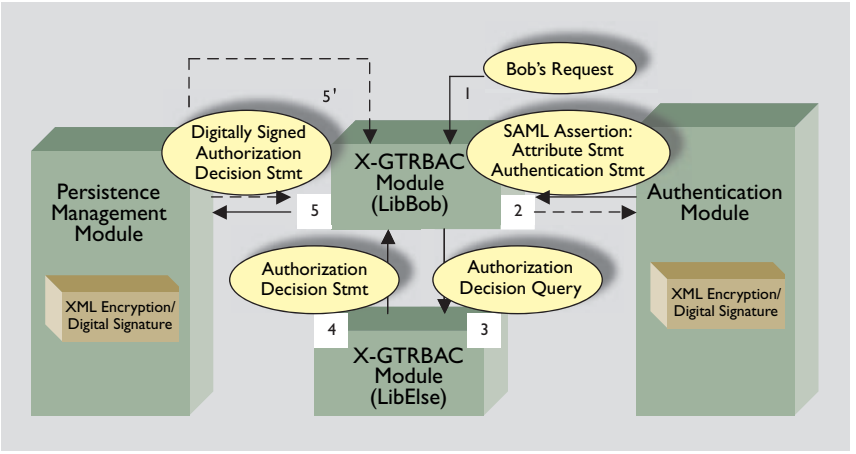

Figure 3. Software architecture for a federated identity- and privilege-management solution.

In addition to TM credential configuration, as specified by the SAML profile for X-GTRBAC, additional requirements affect the use of credentials within the X-GTRBAC system to make it possible to integrate the access control capabilities of the X-GTRBAC system with the Web-based SSO features of SAML.

Role assignment. X-GTRBAC uses the property-based credentials in Table 2 for attribute-based role assignment for unknown users. For example, an appropriate X-GTRBAC policy configuration (see Table 3) allows Bob to access CACM_Vol8_No2 at a federated site (LibElse in the Table) using only his certified attributes. The assignment policy is represented as an XML User-to-Role Assignment Sheet document, as in Table 1.

Delegation. Decentralization depends on delegation and is captured elegantly through role hierarchy in our RBAC mechanism; for example, a junior role inherits all the privileges of a senior role. Our specification today supports delegation only within the role hierarchy; that is, delegation is always from a senior role to a junior role. An optional delegation constraint may be used in the role definition, as outlined in Table 3, to limit the extent of delegation (in terms of time and associated privileges); unrestricted delegation is otherwise assumed. The role definition is given in an XML Repository Systems document, as in Table 1.

Digital signatures. An effective SSO solution depends on the persistence of the authentication and authorization assertions across enterprise domains. Toward this end, the header element of an X-GTRBAC credential includes support for digital signatures. SAML's support for digital signatures allows signed assertions to be exchanged among all SAML-compliant entities.

Software Architecture

Figure 3 outlines the software architecture of this federated identity and privilege management solution. The authentication module is responsible for generating the attribute and authentication statements included in the SAML assertion; standardized protocols allow us to leverage existing mechanisms for these tasks. The SAML authentication request protocol discussed earlier is implemented by standalone SAML-aware Web server software (such as www.pingidentity.com/products/pingfederate.html) and may be deployed by SAML authorities to create and exchange SAML-compliant attribute and authentication statements. The persistence management module is responsible for creating digitally signed authorization credentials.

Our design outsources the credential management to the well-known XML Key Management Specification, or XKMS (www.w3.org/TR/xkms/). XKMS is a Web-based service that can be invoked from a client application and supports PKI-based key generation, registration, revocation, and verification. The Simple

Object Access Protocol binding is used for message exchange. XML encryption and XML digital signature standards provide message confidentiality and authenticity, respectively. End-to-end communication is assumed to be secure by using such mechanisms as SSL/TLS.

The following execution scenario highlights the salient features of the system architecture:

Step 1. Bob logs into LibBob account and requests access to CACM_Vol8_No2;

Step 2. LibBob contacts the authentication module using SAML to obtain the necessary attribute and authentication statements. The authentication module evaluates the information in the SAML request—using either XKMS or the local server—and issues a SAML assertion, including the required statements;

Step 3. LibBob packages the SAML assertion into the evidence element in a SAML authorization decision query, then submits the query to LibElse on behalf of Bob;

Step 4. Based on the SAML assertion in the query, the X-GTRBAC module at LibElse assigns a role membership to Bob (not identified as such by LibElse) according to the available information. The authorization for Bob is determined by the permission assignment policy for the role, and the authorization decision is issued as a SAML authorization decision statement; and

Step 5. To facilitate SSO, the X-GTRBAC module communicates the authorization credential—the SAML authorization decision statement—to the persistence management module, which digitally signs it. Bob can use this credential to access level 2 resources at LibElse without going through an authentication process (step 5).

A preliminary prototype of the proposed architecture is publicly available at cobweb.ecn.purdue.edu/~iisrl/x-access.htm.

Conclusion

This framework is a novel attempt to address the identity and entitlement federation issues we've discussed here. It integrates two security standards—RBAC and SAML—in order to create an access-management specification for open systems. It complements other efforts in this direction aimed at allowing interoperable access management using standard protocols [6]. Our grammar specification supports federated identity and privilege management while meeting the requirements we've outlined. Future challenges include integrating our specification with existing directory schemes to support property-based credentials, trust negotiation protocols for incremental attribute collection, and state information for anonymous users to ensure proper accountability. C

References

1. Bacon, J., Moody, K., and Yao, W. Access control and trust in the use of widely distributed services. In *Middleware 2001, Vol. 2218 of Lecture Notes in Computer Science.* Springer-Verlag, New York, 2001, 300–315.
2. Bhatti, R., Bertino, E., and Ghafoor, A. X-FEDERATE: A policy engineering framework for federated access management. *IEEE Transactions on Software 32,* 5 (May 2006), 330–346.
3. Bhatti, R., Joshi, J., Bertino, E., and Ghafoor, A. X-GTRBAC: An XML-based policy specification framework and architecture for enterprisewide access control. *ACM Transactions on Information and System Security 8,* 2 (May 2005), 187–227.
4. Blaze, M., Feigenbaum, J., and Keromytis, A. KeyNote: Trust management for public-key infrastructures. In *Proceedings of the Sixth International Workshop on Security Protocols* (Cambridge, U.K., Apr. 15–17). Springer, New York, 1998, 59–63.
5. Buell, D. and Sandhu, R. Identity management (guest editors' introduction). *IEEE Internet Computing 7,* 6 (Nov.–Dec. 2003), 26–28.
6. Chadwick, D., Otenko, S., and Welch, V. Using SAML to link the Globus Toolkit to the PERMIS authorization infrastructure. In *Proceedings of the Eighth Annual IFIP TC-6 TC-11 Conference on Communications and Multimedia Security* (Windermere, U.K., Sept. 15–18). Springer, New York, 2004, 251–262.
7. Chadwick, D. and Otenko, A. The PERMIS X.509 role-based privilege-management infrastructure. In *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies* (Monterey, CA, June 3–4). ACM Press, New York, 2002, 135–140.
8. Ellison, C. *SPKI Requirements, RFC 2692.* Internet Engineering Task Force Draft, Sept. 1999; www.ietf.org/rfc/rfc2692.txt.
9. Herzberg, A., Mass, Y., Mihaeli, J., Naor, D., and Ravid, Y. Access control meets public key infrastructure: Assigning roles to strangers. In *Proceedings of the 2000 IEEE Symposium on Security and Privacy* (Oakland, CA, May 14–17). IEEE Press, Piscataway, NJ, 2000, 2–14.
10. Kormann, D. and Rubin, A. Risks of the Passport Single Sign-on Protocol. *Computer Networks 33,* 6 (June 2000), 51–58.
11. Li, N., Mitchell, J., and Winsborough, W. Design of a role-based trust-management framework. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy* (Oakland, CA, May 12–15). IEEE Computer Society Press, Piscataway, NJ, 2002, 114–130.
12. Needham, R. and Schroeder, M. Using encryption for authentication in large networks of computers. *Commun. ACM 21,* 12 (Dec. 1978), 993–999.

Rafae Bhatti (rafae@purdue.edu) is a post-doctoral researcher in the IBM Almaden Research Center, San Jose, CA. This work was done while he was a Ph.D. candidate in the School of Electrical and Computer Engineering at Purdue University, West Lafayette, IN. **Elisa Bertino** (bertino@cs.purdue.edu) is a professor of computer science in the Department of Computational Science and director of research in the Center of Education and Research in Information Assurance and Security at Purdue University, West Lafayette, IN. **Arif Ghafoor** (ghafoor@ecn.purdue.edu) is a professor of electrical and computer engineering in the School of Electrical and Computer Engineering at Purdue University, West Lafayette, IN.