Context-Aware Adaptation of Access-Control Policies

Today, public-service delivery mechanisms such as hospitals, police, and fire departments rely on digital generation, storage, and analysis of vital information. To protect critical digital resources, these organizations employ access-control mechanisms, which define rules under which authorized users can access the resources they need to perform organizational tasks. Natural or man-made disasters pose a unique challenge, whereby previously defined constraints can potentially debilitate an organization's ability to act. Here, the authors propose employing contextual parameters — specifically, activity context in the form of emergency warnings — to adapt access-control policies according to a priori configuration.

Arjmand Samuel, Arif Ghafoor, and Elisa Bertino
Purdue University

In 2005, Hurricane Katrina brought to light shortcomings not only in the US's overall emergency response infrastructure but also in the information-sharing infrastructures necessary to deal with such disasters. The very systems and procedures put in place to protect citizens' information privacy debilitated overall rescue efforts.

One way in which systems cause bottlenecks in rescue efforts is via access-control mechanisms, which, in cases of healthcare organizations, might be implemented to protect privacy by enforcing access-control policies.[1] Such systems allow or disallow access to patients' healthcare information under varying constraints and environments. A rule allowing a physician (identity constraint) to access his or her patient's health records from 9 a.m. to 5 p.m. (time constraint) within the confines of the hospital (location constraint) might provide the necessary patient privacy safeguards; however, it could also prevent an emergency healthcare professional who doesn't have the required credentials from accessing the same records from an emergency location far from the hospital. In most cases, such policies are based on information access for normal day-to-day operations and don't take into account the special needs of natural or man-made disasters. The onset of a crisis demands an expansion of the operating envelope in terms of users, duration, and workplace.

Developing an adaptive access-control

1089-7801/08/$25.00 © 2008 IEEE

system suitable for emergency situations requires addressing many challenging issues. Here, we take a preliminary step toward examining such requirements and outline an approach that automatically adapts an access-control policy in the event of a catastrophic disaster. The adaptation process requires composing alternate policies that would be enforced after a crisis situation was detected. Crisis detection is based on warnings from various government and local organizations, such as the US Department of Homeland Security (DHS) and the National Weather Service (NWS). Relevant requirements for an access-control adaptation mechanism include

- changing temporal constraints, such as the time of day at which users can perform a certain task as well as that task's duration;

The onset of a crisis demands an expansion of the operating envelope in terms of users, duration, and workplace.

- changing spatial constraints to let users access information in emergency locations in addition to in their normal operating environments; and
- enforcing enhanced or relaxed identification and authentication requirements of users authorized to access digital resources.

Our proposed approach addresses these requirements in the form of a context-aware policy adaptation mechanism.

The Proposed Approach

A key issue in developing an adaptive access-control system is adopting a model that takes context information into account. The natural choice in this respect is the *role-based access control* (RBAC) model and its extensions.[2] The *generalized temporal* RBAC (GTRBAC) incorporates a set of language constructs for specifying temporal constraints.[3] *Generalized spatio-temporal* RBAC (GST-RBAC)[4] adds spatial sensitivity to GTRBAC and supports rich spatial constraints. Our current approach to developing an adaptive access-control mechanism uses a feature of GST-RBAC that enables or disables constraints for a given duration or at a specific location as a consequence of runtime events or triggers. We can use *activity context*, or "what is occurring in the situation,"[5] to trigger constraint enabling or disabling. An example is the US Homeland Security Advisory System's (HSAS's) activity context parameter (see www.dhs.gov/xlibrary/assets/CitizenGuidanceHSAS2.pdf), which has five states, or risk levels: low, guarded, elevated, high, and severe.

The constraint-adaptation strategy is the first crucial element in our adaptation approach; to implement it, we categorize constraints into normal constraints (NCs) and crisis constraints (CCs). NCs are defined for an organization's day-to-day operations and are enabled in the policy by default. CCs are specifically defined for operations in case of crises and remain disabled by default, but become enabled during an emergency.

To effectively adapt user authorization in the event of a crisis, we introduce two user classes: weakly enforced users (WEUs) and strongly enforced users (SEUs). The WEUs are users who might already be in the field and might not require authentication during a crisis, whereas SEUs are those who might be responsible for critical information access or actions.

Figure 1 shows system architecture implementing our proposed access-control policy adaptation. We highlight key components' functionality by describing two scenarios, one with a user request under normal circumstances and the other with a user request in a crisis situation.

Access Control under Normal Circumstances

We compose and store access-control policy, including temporal and spatial constraints, in the *access-control policy base*. The *policy instance generator* (PIG) creates an instance of the policy with the NCs. User requests — in the form of time, location, and objects to be accessed — reach the *access-control decision module* (ACDM) labeled 1 in Figure 1. The ACDM decides whether to grant access in conjunction with the *policy instance manager* (PIM), which stores the current policy. The ACDM retrieves the requested object from the *database objects* and sends it to the user (label 3 in Figure 1).

Access Control for Crisis Management

To detect a crisis, the *activity query interface* (AQI) queries the distributed sources of activ-

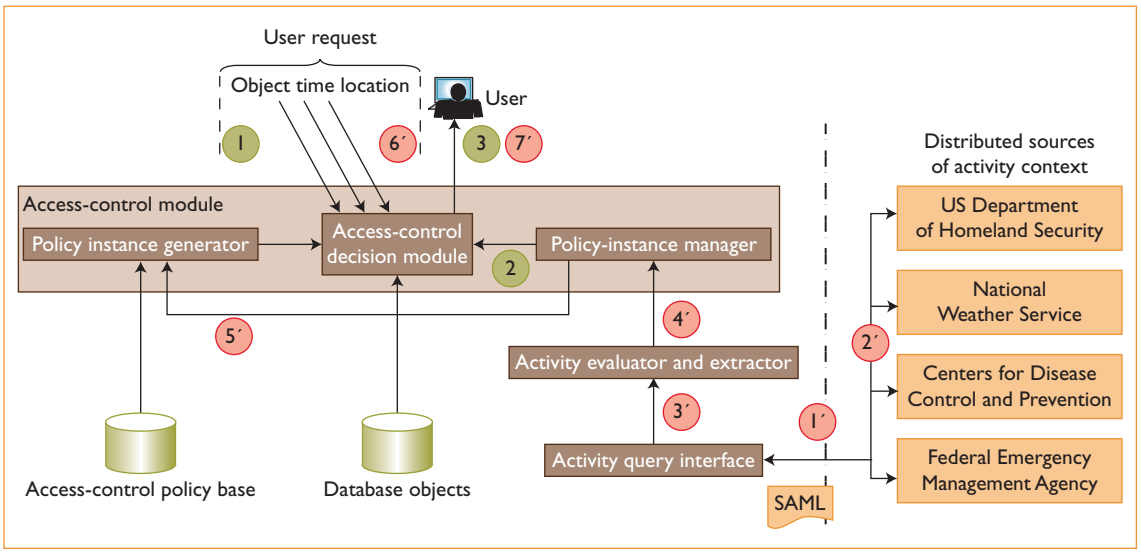

Figure 1. Access-control policy adaptation architecture for crisis management. The system receives inputs from distributed sources of emergency warnings and adapts access-control policies by switching temporal and spatial constraints on or off.

ity context (label 1 in Figure 1). It can base this querying on polling, or AQI can be a passive component waiting for the sources to send out activity-context parameters. Either way, the sources (label 2 in the figure) send out the activity context, and the AQI forwards it to the *activity evaluator and extractor* (AEE). AEE sends individual activity-context parameters to the PIM (label 4 in the figure), which requests a different policy instance based on the activity context's value and the CCs in the policy (label 5). The PIG generates the new instance and loads it in the ACDM (label 6). When the user generates a new request (label 7), the ACDM receives it and grants privileges to the user under a different policy instance.

Research Challenges

Designing and implementing a system of the scale and complexity just outlined requires addressing important research and implementation challenges.

The emergency response enterprise is home to numerous heterogeneous access-control mechanisms — ranging from legacy to advanced systems — with varying features and sophistication. One major challenge is to develop agile and efficient interoperation mechanisms for access-control systems, as well as tools that support real-time policy harmonization. The research challenge in this regard is to design for backward compatibility as well as open standard conformance so that heterogeneous and legacy access-control systems can be included in the crisis management enterprise.

A major implementation challenge deals with the difficulty in foreseeing and composing access-control policies that apply to all possible crisis situations. Catastrophic disasters' huge scale and unpredictable timing — as occurred with Hurricane Katrina and the 2004 tsunami in the Asia-Pacific region — highlight crisis management parameters' inherent unknown nature. Composing access-control policies that encode unknown constraints is a research challenge we might always have to face.

Policy verification, which is a research challenge in any policy-based access-control system, is also an important challenge for access-control adaptation mechanisms for crisis management. We must address policy verification during and after adaptation needs and devise a comprehensive verification methodology for the original policy as well as the adapted one.

Ultimately, we aim to motivate the security as well as the crisis management research communities to join hands and find a novel solution to a pressing need. In this regard, we plan to build a prototype system to implement the access-control adaptation methodology we outlined in this article, and to address the challenges we mentioned.

References

1. S.L. Osborn, R.S. Sandhu, and Q. Munawer, "Configur-

ing Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies," *ACM Trans. Information and System Security*, vol. 3, no. 2, 2000, pp. 85–106.
2. R.S. Sandhu, D.F. Ferraiolo, and D.R. Kuhn, "The NIST Model for Role-Based Access Control: Towards a Unified Standard," *Proc. ACM Workshop on Role-Based Access Control*, ACM Press, 2000, pp. 47–63.
3. J. Joshi et al., "A Generalized Temporal Role-Based Access Control Model," *IEEE Trans. Knowledge and Data Engineering*, vol. 17, no. 1, 2005, pp. 4–23.
4. A. Samuel, A. Ghafoor, and E. Bertino, *Framework for Specification and Verification of Generalized Spatio-temporal Role-based Access Control Model*, tech. report TR 2007-08, CERIAS, 2007.
5. G.D. Abowd et al., "Towards a Better Understanding of Context and Context-Awareness," *Handheld and Ubiquitous Computing*, Springer, 1999, pp. 304–307.

Arjmand Samuel is working toward a PhD in computer engineering at Purdue University. His research interests include context-aware access-control models, access-control policy verification, validation and conflict resolution, and requirement specification of access-control policies. Samuel has a BS in aeronautical engineering from NED Engineering University, Pakistan, and an MS in electrical engineering from the Beijing University of Aeronautics and Astronautics. He is a member of the IEEE. Contact him at amsamuel@purdue.edu.

Arif Ghafoor is a professor in the School of Electrical and Computer Engineering at Purdue University and the director of the Distributed Multimedia Systems Laboratory and Information Infrastructure Security Research Laboratory. He has been actively engaged in research areas related to database security, parallel and distributed computing, and multimedia information systems, and is coauthor of *Semantic Models for Multimedia Database Searching and Browsing* (Springer, 2000). Ghafoor has a PhD in computer engineering from Columbia University. He is a fellow of the IEEE. Contact him at ghafoor@ecn.purdue.edu.

Elisa Bertino is a professor in the computer science department at Purdue University, where she serves as research director of the Center for Education and Research in Information Assurance and Security. Her research interests focus on security, privacy, data management, and distributed systems. Bertino has a doctorate in computer science from the University of Pisa, Italy. She is a fellow of the IEEE and the ACM. Contact her at bertino@cs.purdue.edu.