CHAPTER 34

Panel 2

Reind van de Riet, Raban Serban, Sylvia Osborn, Arnie Rosenthal, Vijay Atluri, Joachim Biskup, Gio Weiderhold

Moderator: Reind van de Riet, Vrije Universiteit, Amsterdam

Members of the panel:

Arnie Rosenthal, Mitre, USA

Radu Serban, Vrije Universiteit, Amsterdam

Sylvia Osborn The University of Western Ontario, Canada

Vijay Atluri, Rutgers University, USA

Joachim Biskup, University of Dortmund, Germany

Gio Wiederhold, Stanford University, California

Contribution by: **Reind van de Riet,** vdriet@cs.vu.nl

The Panel discussed two themes: 1. Are there better ways to protect data from misuse? and 2. Should security be built in at the Applications level? For item 1, in our group we worked on: a) fire walls, objects which are agents, which explode when misused (See Serban's contribution). b) other ways to define access rules: protection in Mokum is provided indirectly by structuring the objects: persons, doctors, nurses, insurance company employees. In this way 90\% of all security is defined. This in contrast to the way security in an ERP system is defined with hundreds of class definitions for thousands of certificates. Another advantage is that security can be proved correct. Item 2 leads in the direction of ERP and WorkFlow systems. In current ERP systems security rules are enforced using a variety of certificates, the possession of which depends on roles persons have in the organization. Using WorkFlows, one can use them for security and privacy protection (See Atluri's contribution).

Contribution by: **Radu Serban,** serbanr@cs.vu.nl
Privacy protection depends on informedness (awareness of threats and vulnerabilities, trust in the technical infrastructure and in the other participants and strict regulations. Apart from legal and technical measures to increase privacy, the designers of future Cyberspace protocols have to consider self-regulatory measures, such as an awareness mechanism based on reputation, a language for specifying scenarios and policies and the adoption of preventive measures. Several principles have been suggested to be enforced by the privacy assistant of an individual: purpose-binding, informed consent, need-to-know (control by source) and appropriate value exchange. In order to increase the informedness of the individual, a model for privacy analysis would require more formal definitions for key notions such as ownership, visibility, responsibility, vulnerability, and provability. In future Cyberspace it is likely that agents representing an individual in an electronic transaction will encapsulate a great deal of personal information and will have more autonomy. Such a privacy assistant has the role of monitoring online transactions, ensuring personal management and keeping the individual informed with respect to his privacy status. It also assesses privacy violation risks, investigates privacy violations and takes corrective measures. We have proposed an architecture of such a privacy assistant, that assists an individual to fine tune the control of his own personal data and keeps him informed with respect to his privacy status. To protect personal information, the privacy assistant has to create and coordinate several user agents, termed fireballs, which encapsulate personal information together with their policies for specific applications. The fireballs cannot enforce protection by themselves, but only function in special trusted environments in which commitments for privacy compliance hold. In this respect, the barriers to effective privacy protection seem to be social, more than technical: the collectors of personal data have to make binding commitments to protect privacy, otherwise software solutions for privacy protection are fundamentally limited.

Contribution by: **Sylvia Osborn,** sylvia@csd.uwo.ca
As a reaction to both themes, I would like to pose the following question: how do different existing software architectures interact with security mechanisms? I think that many newly proposed techniques will not be adopted unless they can be used with existing platforms, existing software architectures and existing software practices. A related question is: can the same security models or mechanisms be used at different stages of the software lifecycle? Is any attention being paid to mechanisms that are appropriate during software development? What tools should be available

and incorporated into software once it is deployed? Are current models/mechanisms adequate for all of these stages?

Contribution by: **Arnie Rosenthal,** arnie@mitre.org
The Grand Challenge is: How can we make enterprise-level administration of security so simple that *ordinary* organizations will do it well? A subsidiary challenge is: How do we modularize the technology, so that vendors will build it? And, what would it take to administer a distributed, heterogeneous, redundant, semi-autonomous system (e.g., databases, business objects, ERP objects) as much as possible as an ordinary system? Discussion: Large enterprises are trying to build systems that make data widely available, in terms of objects that the recipient can interpret (which are rarely the same as those naturally produced by sources). In such architectures, security policies will be specified in detail), examined, and enforced in many positions in a system-databases, object managers, applications (e.g., ERP). Policies will be needed for many derived objects. We need a technical approach that places responsibility where there are both the needed skills (or tools) and the motivation. The best way forward on administration is to provide automated aids for policy propagation and integration and a modular service for each kind of information to be administered (e.g., access permissions, grant permissions, roles, groups, both "info" and "physical" access permissions.

Contribution by: **Vijay Atluri,** atluri@cimic3.rutgers.edu
Workflow management systems (WFMSs) are today used in numerous application domains. The various tasks in a workflow are carried out by several users according to the organizational rules relevant to the process represented by the workflow. Security policies of a given organization are usually expressed in terms of the roles within the organization rather than individuals. With traditional role-based access control (RBAC), roles are assigned to users based on their qualifications, and tasks in turn are assigned to roles, thereby assigning permissions to users. Such a simple model of RBAC is not adequate in WFMS as a full-fledged authorization system should consider the following additional requirements: (1) Permissions should be granted only during the execution of a task, that is, authorization flow must be synchronized with the workflow. (2) Need to assign different roles to tasks based on the outcome of the prior task. (3) Need to grant different permissions to roles based on the outcome of the prior task. (4) Need to deal with authorization constraints such as separation of duties at runtime. (5) Capable to specify different authorizations for different instances of the same workflow. (6) Authorization specification need to be based on the context and based on the responsibilities to be performed by

individuals, and therefore need to be driven by the application. (7) Need for temporal and dynamic role-permission assignment and user-role assignment.

Contribution by: **Joachim Biskup,** biskup@ls6.cs.uni-dortmund.de
We all see the need to build computing systems that are "more secure" than the present ones. We should be careful with our expectations: there is no linear order for "degrees of security", rather we have to deal with several coordinates, governed by specific questions. The most important questions are: 1. Whose security is meant? 2. Which security interests (availability, integrity, authenticity, confidentiality) are affected? and 3. In which application contexts do these interests arise? Further questions deal with costs (in terms of time, space) and willingness of participants to accept the burden of using the security mechanisms? The corresponding coordinates (participants, interests, contexts, costs, acceptance) have to be studied in a common framework. This view on the security problem has some immediate consequences: * Each participant (or each group of participants) needs a toolbox consisting of technical mechanisms each of them is suitable to enforce specific interests in specific application contexts. Unfortunately, such a toolbox is not available yet. * The technical enforcement mechanisms should be composable, interoperable and combinable with application systems. * The effectiveness of the above mechanisms should be founded on a selection of trusted agencies, in order to provide the necessary informational infrastructure. The toolbox must contain "multi-party"-primitives. There are already a few examples, for instance "fair exchange" or "cooperative access rights".

Contribution by: **Gio Wiederhold,** gio@cs.stanford.edu
A novel issue in the security arena deals with protecting children from receiving inappropriate, typically pornographic, content. A law, passed in 1998 by the US Congress, the Children On-line Protection act (COPA), not yet implemented, which makes Internet Service Providers liable for failing to control such transmissions. Hearings on the social, legal, and technical issues have taken place under aegis of a specially constituted commission, which invited a wide range of comments, including organizations outside of the US. Its web page is http://www.copacommission.org/. In October 2000 a final report was released. My testimony can be found at my website. Part of the recommendation included the establishment of green and red top-level Internet domains (TLDs): .kids and .xxx. This November, ICANN (the Internet Corporation for Assigned Names and Numbers) rejected those proposals, mainly because of the problem of assigning authority for those TLDs. For the green TLD, a candidate was the Internet Content Rating Association (http://www.icra.org/), who collects input from volunteer raters.

I know of no such organization for the proposed red TLD. By providing tools for parents and other organizations the actually filtering decisions (who, what, when, how and to whom) can be devolved on people taking a specific and beneficial interest in the issue. At Stanford we have developed a very effective filtering program that recognizes classes of images: WIPE. This technology can support identification of candidates sites for the red TLD. WIPE uses wavelet analysis to extract features from images, and has been trained on pornographic and benign images that are available on the web. WIPE has a recognition rate of 95\% for individual images, and over 99% when identifying porno websites where there are multiple such images.