UCRL-JC-120454
PREPRINT

SCAT: Message Transmission and Retrieval in a Mixed Access Authorization Environment

James A. Guse

This paper was prepared for submittal to the
17th DOE Computer Security Group Training Conference
Milwaukee, WI
May 1-4, 1995

March 1995

Lawrence Livermore National Laboratory

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

SCAT:

Message Transmission and Retrieval
in a
Mixed Access Authorization Environment

Work performed under the auspices of the US Department of Energy by the Lawrence Livermore Laboratory under Contract W-7405-Eng-48

1. Overview

SCAT (Secure Communication And Teleconference) is a communications network providing message transmission and storage services to several DOE communities. It is used for both routine and emergency communications in an environment where not all users have formal access authorization to all data on the system. The network consists of a Central Computer server located at LLNL to which remote Windows™ GUI-based client PCs connect, currently using STU-IIIs over dial-in phone lines. All data resides on the Central Computer and can be retrieved by authorized recipients at any time. The Central Computer authorizes all access to the data, and remote workstations are completely untrusted.

SCAT is designed to handle unclassified information and classified information up to the SECRET level. All users of the system must hold a DOE "Q" clearance or equivalent (i.e., authorized access to Restricted Data); there is no provision for multi-level access, although from an architectural and implementation standpoint support for multi-level access would be straightforward. The rich security architecture of the system derives from its handling of the intelligence community markings or "caveats," NOFORN, WNINTEL, NOCONTRACT, ORCON, and PROPIN, as well as the DOD control CNWDI.

Each remote workstation is approved for a specified set of caveats, based on the approvals for the facility in which it is located and the needs of the group or program using it. In addition, each remote workstation user is authorized access to some (possibly all) of the aforementioned caveats. Because the information processed by the workstation must be compatible with the access authorizations of the users who will routinely access it, in practice, the lowest-common-access-authorization of the Workstation and all its users determines what SCAT access authorizations are given to its users. This is accomplished through a combination of administrative and software-based checks and controls.

The users of each remote workstation are grouped into an organization and given a distinct organization-ID. Typically, there is a one-to-one mapping between SCAT Workstations and organizations; however, there are cases where a single organization has multiple Workstations (either for convenience or to support different access authorization profiles). The need for single Workstations to be associated with more than one primary organization-ID has not arisen, except within the LLNL SCAT Project group.

Data on SCAT is organized into mutually exclusive Events. Within an Event users create Documents of one or more different styles, and Documents of a particular style are numbered consecutively within the Event. Different styles may contain different types of data, including ASCII text, graphics, and unstructured bytes. Multiple styles containing the same type of data (e.g., ASCII text) are used when each style has a distinct purpose (e.g., formal announcements versus informal discussion). Events are generally created to support ongoing discussion or announcements related to a general topic, or for discussions and other communications related to a specific real-world emergency or threat. We discuss the security-related attributes of both Events and Documents in more detail below.

One reality with which our design must contend is that the information transmitted over SCAT is often sent by and intended for people who do not have actual on-line access to the system. Therefore, the access and routing controls implemented in the software are intended only to complement and facilitate comprehensive procedures for controlling and disseminating classified information and documents in the real world.

2. Mandatory versus Discretionary Access Control

SCAT defines Need-to-Know as a formal equivalent to the real-world concept by the same name. A responsible manager determines Need-to-Know for access to an Event, and a Document's originator (or authorized modifier) determines Need-to-Know for access to each Document. The SCAT Management Staff maintains the list of organizations with a Need-to-Know for the information in an Event. A Document's creator addresses the document to some (possibly all) of the organizations (and/or users) in the Event in which it is created, thus defining the Need-to-Know set for the Document. By definition, all users within an organization (as specified by an organization-ID) have a common "need to know" for information routinely set to that organization.

Access control based upon Need-to-Know is termed discretionary access control. SCAT also implements access control based on caveat labels and access authorization, which we term mandatory access control. System users are not at liberty to override these controls (except perhaps by improperly labeling a document).

Conventional definitions of mandatory access control assume that both the access authorization of the subjects (users) and the labeling of the objects (Documents) are controlled exclusively by the trusted system. Such systems label all objects with the maximum access authorization of the subject creating (or modifying) it. This model is impractical in a communications system since it would prohibit the sharing of information between subjects of different access authorizations. To overcome this paradox, SCAT relies upon human operators to correctly label the documents they create. Since any classified document must undergo an ADC determination before being placed on the system (and the user must enter the relevant ADC information), there is a high degree of confidence that the entered labels will be correct. Furthermore, the worst-case scenario of incorrect labeling is the disclosure of a caveated document to an unauthorized individual. DOE felt that this risk was low enough to be acceptable, in light of the system's auditing facilities and training program. Were SCAT to be a multi-level system, with users having different clearance levels, it is likely that the risk of unauthorized disclosure would have to be mitigated in additional ways.

3. Event Access Control

Each Event has a list of organizations authorized to access it. An organization's membership in the Event access list is determined by the Event's responsible manager and defines the generic Need-to-Know of that organization's users for some of the information within the Event. Users in an organization without access to a given Event will never know of its existence. Furthermore, two organizations will nominally not know of each other's existence on the system unless they share access to at least one Event.

Each Event has a minimum and maximum classification level, as well as a (possibly empty) set of forced caveats. The allowable classification range for the Event is primarily a user convenience. It can be used to define "unclassified" Events for training and testing, as well as to force all discussions within an Event to be held at a minimum classification level.

Forced caveats cause all documents created within an Event to be labeled with the specified caveats. They also preclude

access to the Event by users (and/or organizations) who lack authorized access to all forced caveats on the Event.

Each Event is assigned a Coordinator organization, that has an implied Need-to-Know for all Documents in the Event (regardless of the Document-level discretionary access control) as well as the ability to re-address most Documents within the Event. Select trained and certified users within the Coordinator organization are authorized these privileges.

4. Document Access Control

Each Document's originator specifies an addressee-list defining those users and/or organizations with a Need-to-Know for the Document. The originator may designate one or more addressees who are allowed to create a new (slightly modified) version of the Document (including a modified addressee-list).[1] Although the capability exists to address documents to individual users, such narrow addressing often results in information not reaching the addressee in a timely manner and is generally discouraged.

A Document's originator also specifies the classification level, category, and caveats of the Document. These labels are subject to any Event-imposed constraints. Administrative and procedural controls assure that Documents are labeled properly both when entered onto and removed from the system. Authorized modifiers may specify different classification and caveat labels for the new version of the Document they create.

It is possible for a Document to be addressed to a user or organization that lacks the caveat access authorizations to see it. In this case, the intended recipient is given an indication that the Document exists, but that they lack the necessary authorization to retrieve it. This approach allows the recipient to notify the originator of the problem and have the originator either (1) remove that recipient from the addressee-list, (2) obtain the necessary access authorization for the recipient, or (3) make a sanitized or downgraded version of the Document available to the recipient.

5. Intelligence Information and ORCON Caveat Handling

"Intelligence information" is subject to the special requirement that it may not be released outside the

---

[1]Only the originating organization may modify a document labeled with the ORCON caveat.

Intelligence Community without the consent of the originating agency. While the meaning of Intelligence Community is well-defined, the meaning of "intelligence information" isn't. SCAT approximates the intent behind this restriction by labeling each organization as belonging to the Intelligence Community or not, and by labeling each Document as being Intelligence Information or not. A Document is considered to be Intelligence Information if it is classified, and either (1) has one or more of the intelligence caveats applied, or (2) was originated by one of the (few) organizations designated as "generating intelligence information." Typically, the intelligence-producing agencies in the Intelligence Community are so-designated because most of the information they introduce on the system is "intelligence information."

ORCON is a somewhat special caveat in that rather than representing a blanket access authorization, it is applied to a document by an originator whose permission must be obtained prior to disseminating the document further than the originator explicitly specifies. In addition to imposing additional restrictions on how a document may be routed, the ORCON caveat is treated within SCAT like other caveats for purposes of access control, allowing certain users and/or organizations to be denied access to all ORCON Documents.

In the real world ORCON documents are created by intelligence-producing organizations. Generally, these sources do not directly enter such documents onto SCAT. Typically too, since the intended recipients of documents transmitted over SCAT often do not have on-line access to the system, the originator's intended dissemination cannot be accurately represented in the Document's addressee-list.

To approximate the desired functional behavior, the addressee-lists of Documents marked as ORCON may not be altered except by the originator. The addressee-lists of Documents marked as Intelligence Information may not be altered to include users and/or organizations not in the Intelligence Community except by the originator. The originating SCAT user/organization is responsible for obtaining any necessary ORCON or intelligence information release from the originating authority.

6. Beyond Caveats

An important generalization of the access control model in SCAT is to permit the definition of access controls for information to which the SCAT Management Staff does not have authorized access. Such information typically exists within special access programs, which are increasing in popularity. We have considered two basic approaches to

this problem: the first assumes that such accesses would be modeled much like existing caveats (a "Special Access Control"), the second assumes that special access would be controlled by virtue of access to an Event (a "Special Access Event").

Both approaches must rely on the use of a public-key encryption scheme to protect a Document encryption key, and both allow a remote Workstation site to administer the special access granted either to users and organizations or to Events.

In the Special Access Control case, the remote managing workstation would be responsible for authorizing special access on a per-user basis. In the Special Access Event approach, it would be responsible for managing an Event.

To support either approach a remote Coordinator organization must be able to securely distribute encryption keys to authorized organizations (and/or users). Consider a public-key encryption system where each organization (and/or user) holds a private key whose corresponding public key is stored on the Central Computer. Upon initially gaining access to the system, each organization (and/or user) creates a public/private key pair. By retrieving the public key of an intended recipient, a remote coordinator organization could encrypt a message and send that message to the intended recipient. Such a message might contain the access key for a single Document, or for all Documents within a Special Access Event or covered by a Special Access Control. Finally, all Documents to which the Special Access Control is applied or which are created within the Special Access Event, would be encrypted such that only individuals with the appropriate authorization could decrypt them.

While the Central Computer could still represent and authorize access as it currently does, the granting of access by the Central Computer (which is under the control of the SCAT Management Staff) would not give access to real data, only to the encrypted form of the data. Since the SCAT Management Staff does not possess (nor can they legitimately obtain) the key that would enable them to decrypt a protected Document, they would be denied access to the (decrypted) content of all Special Access Documents. Furthermore, the managing Workstation must digitally sign the authorization information stored on the Central Computer, so that all authorized users can rely on it.

There are a number of outstanding issues with either design, including: the granularity of public-key issuance (i.e., per-organization, per-user, or both), how to protect the private key(s) on each remote workstation, validating that the Workstation software (whose implementation is still

under the control of the SCAT Management Staff) implements those protections correctly. There is also not clear precedent that software-based encryption would be approved to protect special access information in a common-clearance environment. And finally, introducing the Workstation as a trusted (and mutually suspicious) component of the SCAT network alters the security assumptions of the system in a fundamental way.

One key advantage of the Special Access Control approach would be the ability to apply any combination of controls to any document. Whether this would prove particularly useful is dubious, since special access programs are by design separate and compartmented, not overlapping and combined. Another advantage is an enhanced ability to grant and later deny access to individual users, since the mandatory access control model already provides for this. It would be cumbersome (or require additional functionality) to manage per-user access with the Special Access Event approach.

Because the current SCAT architecture already supports having a remote Coordinator organization for an Event, it is a minor change to permit that organization to exercise complete control over the Event. It would considerably complicate the SCAT security model to offer each of many remote workstations the ability to control certain access authorization rights within each user's and organization's profile (as well as possibly each Event's "forced special-access-controls" attribute). The user-interface would also be more error-prone and less friendly if users were required to select from a myriad of special access labels to apply to each document, rather than have all communications automatically protected by virtue of being in a Special Access Event.

7. Conclusions

SCAT demonstrates the feasibility of a user-friendly communications tool in a mixed access authorization environment. It offers decided advantages over point-to-point solutions, which do not provide a shared archive. As special access programs increase in popularity, communication using a shared archive, while not granting the operators of the archive access to all data contained thereupon, will become an increasingly sought-after solution. SCAT is well positioned to be a baseline for developing such a solution.

James Guse received a B.A. from Hood College (Frederick, Maryland) in Mathematics and Computer Science and a M.S. in Computer Science from U.C. Davis. He is currently the SCAT Project Leader in the Response Technology Program at Lawrence Livermore National Laboratory. He has been with LLNL for the past seven years where he has worked in the area of networked and distributed systems.

Technical Information Department • **Lawrence Livermore National Laboratory**
University of California • Livermore, California 94551