Part 12: System Security

Page 1

We are finally back after a busy fall with another installment in our series on court case management systems. In this installment we discuss CCMS system security design considerations.
Individual Identification and Authorization

Picture CCMS 11

The User

Any security system begins with the user. Identification of a user and subsequent registration to provide credentials (username and password) are a normal part of system administration. However, assignment of security access may depend on the role that the person performs in court. Obviously a judge has a high level of access compared to, say, anew court clerk. So management of the person's access connects to two areas: their position title managed by human resources (HR) and their work assignments that are managed by court management (presiding judge/ elected or appointed clerk/ court administrator).

Automated CCMS will support both requirements. Some advanced courts have connected their automated CCMS with their human resource systems via LDAP2/LDAP3 protocols (see end note below) that provides an ongoing automatic verification that the person is still employed by the court and holds a particular position as defined in the personnel system. This automated connection is extremely handy for large organizations and relieves the system security administrator from one more worry, not being notified of a person ending court employment. Of course the HR system does not track what a person's work assignments are in the court and, hence, the information they need to access. This must be performed by their work supervisors and transmitted to the CCMS security administrator. The more efficiently this is communicated, the easier it is to have a secure system.

Roles

The definition of role in a CCMS is both court staff assignments as well as case participants. Therefore, in each case, people have roles and relationships to case types, documents, and data. And specifically work roles will vary based on the case, case type, court, the court organization, and the organization of case participants.

For example, within a court, a court work role might be to accept incoming cases (and all the work that entails), while others are scheduling hearings or presiding at hearings or trials. Thus in a small court one person will have multiple roles while in a large court one person will have one role. We see this in many places where a judicial "commissioner"may do nothing but criminal release hearings as their job, while in a small court the judge performs this among many other judicial functions.

And roles change. A person may have their work role for a specific time period before it changes according to business and personnel needs. Thus, the CCMS should capture the start and end date for the person's role assignment in a history of work assignments.

Another common requirement for CCMS is to track judicial conflicts with case parties and/or attorneys. The role that a person has in a case, as well as the type of proceeding that the judge is assigned, may determine whether a judge should be disqualified or not.

And yet another example of the role is an attorney who was involved in a case early in his/her career, say, as a prosecutor, but now has become private counsel. They may not be able to access case information, for instance, in a juvenile matter that they prosecuted in the past, now that they are in a new role in relation to the court. This type of information is most effectively maintained in a table of conflicts that may change from time to time conflicts are discovered and resolved.

Groups

A related security access concept is groups. A group in a CCMS will be a court, the members of the judicial chamber, or a clerk/ registry office.

And for example in litigation, a case may have multiple plaintiffs/ petitioners and multiple defendants/ respondents (claimants). These parties, counter-claimants, cross-claimants, and third-party claimants may be involved only as to certain claims, so all parties involved in motions concerning certain claims need to be noticed for court events orbe sent court orders. As certain claims are amended, adjudicated or settled, systems need to track the status of those claims and which parties are involved.

These examples show what everyone in the legal system knows -- relationships and groups are dynamic and complex and therefore must be managed. In CCMS, group membership often sets the "floor" for access to data. Simply having a role of a judge or clerk/ registrar results in default access. And while this level is fine in most cases, because access can also be controlled by the computer's location in a building on a network, it provides only the most basic filter. And in our experience, access allowed by statutes and courts rules and changes of roles within organizations generally require more granular control.

Trust

The concept of trust was explored in this earlier CTB article on Trust and E-Filing that dealt with information access from outside the court organization and between trusted justice agencies.

Internally, trust is another matter. To quote President Reagan (apparently based on the Russian proverb he learned), the operative approach is "trust, but verify." Access to data is required to operate the court. But in order to identify, and constrain, abuse, robust logging must be built into the system. And since courts must account for money received for costs, fees, fines, bonds, and other trust accounts, appropriate data logging along with standards-based procedures must be

implemented.

Now if we have done a good job in identifying the person using the system, we can log what they did in the system. In the past this was often not feasible because of the amount of storage needed for the logs, but with computer disk capacity being literally pennies per gigabyte, that barrier has been eliminated.

Logs can also include network and machine information in addition to the user's account to identify when and where the data was entered. Many systems use the computer network card MAC address for this purpose.

The question then becomes who audits the logs? In some courts it is done as part of the financial and process audit review. But in others it is up to court management to perform this duty.

Therefore, it behooves the CCMS designers to provide a rules-based audit portal to facilitate auditing by the court manager or other role. And if a problem is suspected, the audit portal should facilitate a trained forensic data system auditor's further investigation of the full data set.