Panel 4: Secure Audit
Chair by Carl Gunter, University of Illinois at Urbana-Champaign
Panelists: Laurie Williams, North Carolina State University; Kai Zheng, University of Michigan; Joe Lorenzo Hall, New York University; Bradley Malin, Vanderbilt University; Soumitra Sengupta, Columbia University

Summary of the Panelists’ Presentations and Panel Discussion
Auditing is a widely employed approach to detecting and deterring access abuse for EHRs (electronic health record systems). This panel explored the issues relevant to current auditing techniques and proposed methods aimed towards mitigating these issues.

Carl Gunter began the session with a brief introduction. In the hospital settings, people have a job to do and there’s a complex workflow. Since it is difficult to predict who needs access, least privilege is difficult or impossible to maintain; instead accountability and good judgment are assumed. This accountability-based model is well entrenched, but, unfortunately, increasing scalability of electronic health records invites a host of new threats.

In the current model, one collects an audit, shoves it in the closet, and if someone complains, the audit is examined for evidence regarding the complaint. This is an ad hoc approach that is not suitable to current problems like large-scale identity theft. The hope is to get around this reactive model and shift to a proactive model to better respond to emerging threats.

Soumitra Sengupta then spoke about audit logs at a large tertiary care facility where he works. He worries about big spills that may emerge from hacking, but he feels that non-compliance with government regulations is the biggest risk he faces. The risk of leaking data is tremendous. On a smaller level, there's the risk of celebrity snooping and acquaintance snooping. Audit logs provide solutions to these problems. While he has not seen any large-scale problems anywhere near the level of identity-theft, one issue is a lack of standards in audit logs. HIPAA says that logs should be used, but doesn't specify much about the details. There's a guide to computer security log management (NIST 800-92) and also an ATNA standard, but these are inadequate. The punch line is that there is no useful standard that is followed. But there's a strong need for one.

Next, Bradley Malin discussed the relevant problems in audit logging, EBAM (Experience-Based Access Management), and future worries. Tensions between two schools of researchers, audit experts and access control policy setters, pose a major problem. There are many papers on role engineering, but they have little use in practice due to the necessity for and requisite amount of human-human and human-computer interaction. Eliciting the correct roles and permissions from humans is almost impossible to do in a fine-grained manner. Also, jobs and responsibilities are not well documented and people are generally poor at providing documentation off the top of their head. This is the impetus that drives the design of EBAM, which looks at how experience with access to sensitive data can be used to inform access privileges such as role definitions and assignments. EBAM envisions a contrast between an ideal model with the access permissions that the organization (ideally) intends and the enforced model that comprises the rules that the computer systems actually impose. Audit
logs inform the gap between these models and support the development of an expected model that can be used to improve least privilege over time. And this system continues in a cyclic process, continually improving until some equilibrium between the envisioned model and the constraints imposed by reality is reached.

There are multiple ways to harness the information in audit logs. The key is coming up with an effective way to pull out lots of different patterns and employ these patterns to enforce the rules. Numerous problems must be overcome: different providers within the same ward have different behavior, different wards within the same healthcare institution have different behavior, different healthcare organizations have their own way of logging, and there is a dire need of harmony and interaction between logicians and access control policy setters and machine learning experts.

Laurie Williams spoke about secure logging and audits. Recently her students have been working with her in coming up with software engineering techniques to apply to healthcare. One major concern is the threat of personal records being stolen. A primary issue they felt should be addressed dealt with peeking; audit logs could serve to manage the situation.

She did studies with three extensively used systems, which are now certified applications, but weren't at the time. The team wanted to look at how well information is logged when data is created, edited, and deleted. They looked at the CCHIT criteria, but couldn't get the system to work as the functionality simply wasn't there. Sixty-one percent of the time actions were performed that should've been recorded in the audit log, they were not recorded. Actions that should not have been performed were done without a trace. So, there's tremendous concern.

Her team also developed an application for patients called iTrust that notifies patient when their data is accessed in illicit ways.

Kai Zheng followed with a short discussion on how to improve the workflow in hospitals. It was premised on the assumption that if one can understand the complex workflow in a system, it would be easy to predict what people will do and detect people who would abuse the system. He talked about how the audit trail is not limited to access logs; there's more information that must be included such as clinical content, timestamps, determining the person who entered the data, and the database. Integrating these pieces of information together with the access control logs provides a more comprehensive picture of what's happening.

There are many difficulties human auditors have in evaluating the authenticity of potential threats. It may be hard to distinguish malicious intent from normal behavior, and it's not always obvious who the bad guy is. Ergo, a better approach is needed. One involves the recognition of collaborative access patterns wherein a sort of social network can be constructed from the audit trail. Another is intent-driven workflow pattern recognition. Here, hidden patterns embedded in the audit logs can be detected by machine learning techniques to predict what people intend to do.

Joe Hall wrapped up the session with a discussion of policy. Patients should know how their information is being used and disclosed. However, patients don't appear to be using accounting of disclosure right now, possibly because patients don't understand them. It would
be helpful to involve patients directly in auditing. What do patients care about? Why not aggregate audit logs across institutions to allow for comparisons? This could also be used as a complement to the accounting of disclosure. In sum, there are numerous problems and unanswered questions in regards to privacy and enforcement issues.

The takeaway is that there is a lack of standards, an archaic model of reactive logging, insufficient involvement of patients in the design of systems, and numerous policy and enforcement issues. These factors contribute to significant problems with the current approach of audit logging. In response, access control methods like EBAM, tools like iTrust, and machine learning techniques to detect abuse are being developed to counteract these concerns.