Evaluation of Audit Trails and Security Features in Software Systems

INTRODUCTION

As laboratories are becoming increasingly dependent on software systems for forensic DNA data analysis, audit and control features are becoming more crucial. Analysts and laboratory directors are finding that software systems, in addition to being user-friendly, must also provide an adequate level of security and control features in order to ensure that any changes or edits made to a project can be traced back and validated. It is becoming more evident that software programs that disregard security features or are vulnerable to outside intruders may put the laboratory at risk.

As a result of the NIST NEST Project Implementation Team’s recent efforts to standardize software systems, a laboratory director is now required to review and evaluate software for application to forensic DNA laboratories. Each software program must provide a unique profile for each scientist, and all changes made to software should be logged and stored in an audit trail. The laboratory must be able to identify who made edits to software systems and when, as well as the purpose of the edit. This is necessary to ensure that all changes are recorded and that security and quality assurance measures are in place. The data analyst is required to record the time that specific changes were made to the software, as well as the analyst’s unique user id and password.

As a user, does the software ask for a user id? 

As an administrator, do you have permission to read the analysis method, but not permission to update the analysis method? 

The expert systems and mixture deconvolution tools evaluated by the NEST Project Implementation Team have features that offer a wide variety of benefits to forensic laboratories. Our evaluation of the different software systems demonstrates a need for similar regulations for e-signatures may arise. If enough security measures are implemented, then those signatures offer a wide variety of benefits to forensic laboratories.

The forensic science community is making strides towards a paperless system. As this movement progresses, the role of electronic signatures (e-signatures) becomes a concern for the laboratory. As a result, every project during DNA analysis and computer software programs must provide a unique user id and password to login to the software. Without these, the software will not open. In addition, laboratory directors must evaluate software systems for their ability to track and/or store login information. Table 1 shows a brief summary of each program that was evaluated.

MATERIALS & METHODS

Output files were examined for security features. Security and audit trail features were recorded when encountered during sample processing.

RESULTS

Table 1 presents a summary of features evaluated within each software program. The table includes the results of the evaluation of each software program in terms of security features.

<table>
<thead>
<tr>
<th>Software Program</th>
<th>Description</th>
<th>Security Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>GeneMapper</td>
<td>Analyzes DNA samples</td>
<td>User login and password required. User ID and password must be entered for each analysis.</td>
</tr>
<tr>
<td>ID-X</td>
<td>Tracks the Windows® user login. A user ID must be entered for each login.</td>
<td></td>
</tr>
<tr>
<td>STRess</td>
<td>Tracks the Windows® user login. A user ID must be entered for each login.</td>
<td></td>
</tr>
<tr>
<td>STRess-Analyzer</td>
<td>Tracks the Windows® user login. A user ID must be entered for each login.</td>
<td></td>
</tr>
</tbody>
</table>

ACKNOWLEDGEMENTS

The authors of this paper would like to acknowledge all members of the NEST Project Implementation Team for their support and assistance with this project, specifically Chuck Heurich, Program Manager to the NEST Project. The authors would also like to thank the National Institute of Justice, the U.S. Department of Justice, and the Forensic Technology Evaluation Center (FTCoE) as the host site of the NEST Project.

REFERENCES