Murray, Meg Coffin (2010). Database Security: What Students Need to Know
Journal of Information Technology Education-9.(2010), Innovations in practice IIP-61-77, *Faculty Publications* at Kennesaw State University.

Article Summary

Problem:

What is the current outlook on database security, What topics do students need to know about in a database security course, how can these topics be taught effectively?

Goals:

Present statistics for data breaches. Highlight the gap in knowledge students who take database security courses, as the database security knowledge base continues to grow. Describe essential sub-topics that may be included in the curriculum of these database security courses. Introduce and review an interactive learning tool, to reinforce the courseware in more effective ways.

Specific Research Questions: (Critical)

- What is the current industry census for data breaches?
- Is the present database security curriculum enough for students of computing disciplines?
- What are some mechanisms for securing data that can be included in the curriculum of database security courses?
- Discuss relevant sub-topics from database security courses.
- Discuss the possibility of a better medium to reinforce data security courseware.

Hypothesis:

There does not appear to be any hypothesis mentioned for this research study. The article by Meg C. Murray seems to be seeking answers, to the question above; it describes an ad-hoc enhancement that may augment the effectiveness of the current approach. The article does not seem to have any preconceived notions about what the ideal solution should be.

Design and Procedures:

The design of the article by Meg C. Murray (for evaluating student perceptions of the teaching effectiveness of the Security Module) was to conduct an online questionnaire for sixty students, the thirty-eight students who responded to the survey were interviewed by the faculties who used this courseware in their classes. The students were then asked to assess the sub-modules of the software. After the assessment, the students were asked to comment on the effectiveness of the sub-modules and their learning motivations. Faculty reports were also taken concerning how their teaching efficacies were affected. This evaluation was limited in scope to a small number of students and faculty.

Results:

- 38 out of 60 students responded to the online questionnaire; Three faculty members interviewed these students.
- Majority of students that is, more than 19 students, indicated that they agreed or strongly agreed that the sub-modules enhanced their learning.
- SQL injections and row-level security received the highest 'positive' ratings from students.
- Database inference and database auditing received the highest number of students reporting a rating of 'neutral.'
- 41% of students were motivated to use the software when their instructor had explicitly specified it.
- 51% of students reported using the software on their own.
- 8 % of students reported that they used the software often.
- Most common reasons for using the software was "to complete homework assignments" or "to study for exams".
- Faculty reported enhancements in teaching and cited that the courseware mapped well to the class-concepts taught in class.
- Faculty also cited that the coursework was much better for presenting the concepts than the traditional way of drawing pictures on a whiteboard.

Conclusion:

In conclusion, It had been made evident that computer and database systems need to be secured, and it has been emphasized how securing data must be part of an overall computer security plan. It can also be concluded that interactive learning is conducive to the exploration of database security issues by students, and it also helps in identifying practical implementation methods to database security mechanisms.

Article Critique

Introduction:

This is a critique of the article "Database Security: What Students Need to Know" by Meg C. Murray[1]. The article is primarily concerned with a) Growing concern and the need for data security; the importance of protecting data. b) Overview of sub-topics in database security that can be included in database security courses: access control, application access, vulnerability, inference, and auditing mechanisms. c) Reviewing a tool to enhance the effectiveness of teaching data security topics. The article references "Teaching Database Security and Auditing", by Li Yang[2] a similar article which focuses on the same sub-topics but instead of animated courseware it focuses on introducing hands-on laboratory sessions to implement various techniques of the securing a database, as part of the curriculum to impart to the students - some real-world experience database security experience

Abstract:

The article asserts that there is a growing concern for database security which can be evidenced by an apparent increase in the number of reported incidents of data loss. The article mentions statistics of multiple data breaches reported by The Privacy Rights Clearing House, Ponemon Institute, and The Verizon Business Risk Team. The referenced article by Li Yang also cites reports by FBI and Amazon.com. The findings in these reports reveal that majority of data breaches have resulted from hacking techniques such as SQL injections, and malware targeted on errors in the database and unauthorized access; the article mentions that the breaches could have been prevented with some efforts. By citing facts and figures from reliable sources, the article has tried to highlight the need for data security. The article further states that achieving data security is simple, but the path is not that simple. Inadequacy of traditional systems is described as one of the culprits behind increasing numbers of data breaches. The rationale could have been better substantiated by providing some intrinsic detail here.Next, the article emphasizes on the advantages of software animations and how they can leveraged to convey topics effectively in database security courses. A tool named Animated Database Courseware (ADbC) has been developed by Kennesaw State University under a National Science Foundation Grant and made available free of cost. the article will use ADbC as a medium to test the efficacy of software animations as it has claimed. The article has identified access control, application access, vulnerability, inference, and auditing mechanisms, as the essential sub-topics that need be covered under an introductory database security topic in a given course, in the referenced article by Li Yang seven lab modules are designed to cover database security. The author has justified the reason for not including all the relevant sub-topics for database security, the focus is limited to mechanisms for securing data, hence only five modules were included.

The author defines access control as a way to restrict access to the system by assigning rights and privileges to specific data objects and data sets in combination with authentication and authorization; the author then sheds light on three ways of defining it: Mandatory Access Control (MAC) Discretionary Access Control (DAC), and Role-Based Access Control (RBAC). The author has contrasted depicted contrast in these ways, MAC is system defined and static, DAC is user-defined and dynamic, but RBAC is a better combination of both, and most efficient of the lot. The referenced article by Li Yang, also mentions that Role-based access control (RBAC) is an alternative to traditional DAC and MAC and attracts attention from commercial applications. The referenced article further explains that Users authorized to powerful roles do not need to exercise them until those privileges are actually needed. This minimizes dangers due to intruder masquerading or Trojan Horses, and it also talks about Virtual Private Databases(VPD) that provide row-level access control in addition to user-level and role-based control. The article by Meg C. Murray also talks in brief about row-level control but does not mention anything about VPD; Still, the overall explanation is appropriate and good enough.

The article then describes Application Access Management and explains how a security matrix can visually help in identifying the correlation between the operations performed on a database the authorizations needed for database objects. The author has further highlighted that visual depiction of data integrity rules, makes it easy to identify all application programs potentially affected by any change made to a database table. Meanwhile, the referenced article by Li Yang, very briefly talks about SQL injection in the context of application security. The author Li Yang states that, by entering malformed text data in the commands sent to an interpreter, the malicious user can either gain access to unauthorized information or alter the data in the database, this is termed as an SQL injection. The article by Meg C Murray, has established SQL Injections as the most publicized Database vulnerability and talks more about the conventional ways of preventing SQL injections by addressing query string validation approaches i.e.. *Black List, White List and Parameterized queries*. Both the article provides a visualization of SQL injection using the ADbC tool. It hints towards the efficacy of animated courseware, as was asserted by Meg C. Murray.

Next, Meg C. Murray discusses Database inference as the ability to infer unknown information from retrieved information. It states that inference often happens in cases where the actual intent is for users to generate or view aggregate values when they have not been given access to individual data items. The author has stressed that there are no ideal solutions to Database Inference. The only solution that is recommended by the author is to include controls related to queries or individual items in a database. Database inference is not covered in the referenced article by Li Yang. The reason for mentioning database inference is to focus on how important it is for students to understand the occurrence and risks of inference. Substantial research has been done for the problem of statistical disclosure control, but still, there are no significant developments to solve this problem. In my view, it was a great idea to mention Database inference, because, without awareness of the problem, it can persist for a long time.

Finally, the article by Meg C. Murray seeks to establish database auditing as a way to identify if breaches have occurred rather than preventing the breach itself. The author categorizes audits as an activity tracker for Data Control Language, Data Definition Language, Data Manipulation Language and logon/logoff attempts. The referenced article by Li Yang describes two more categories to audit changes to sources of stored procedures and triggers where malicious codes can easily hide. The sixth category is to audit database errors because attackers will make many attempts before they get it right. The author Meg C Murray fails to address many important details here, and this is where I do not wholly agree with the article. During massive attacks, the hackers often target and modify audit tables itself, and even erase system logs to stay untraceable and be able to repeat attacks. Often, the breaches do not end in one day but persist for weeks or even months, and if the attacker can gain root access, the logs can be disabled and wiped clean in a few clicks.

Results:

It can be concluded that the evaluation of student perceptions of the teaching effectiveness of the Security Module was positive for most parts. The article by Meg C. Murray asserts that the majority of students indicated enhanced learning; it also reveals that 51% showed enough motivation to use the software modules on their own. 8% indicated they used the software often. It further states that Faculty members also reported enhanced teaching experience by the courseware. Still, since the evaluation was limited to only 38 students, and the majority of students means just 20 students. Hence, the results do not reflect on how the assessment will turn out if the demographics are changed. Overall it is accurate to say, and proven multiple times that the use of animation helps augment learning. The article by Meg C Murray makes an excellent introductory resource for someone taking their first steps into database security.

Discussion (Things I Learned):

The overall takeaway from the article by Meg C. Murray and reference articles are as follows. Some ideas of further study are presented in the referenced article by Li Yang.

1. The extract from article by Meg C Murray "A simple tool, known as a security (or CRUD) matrix can be used to explicitly identify the required access rights needed by an application program. Specifically, the security matrix provides a visual depiction of the correlation between the operations or authorizations needed for database objects and input/output sources such as forms and reports."
2. The article by on Dynamic Inference Control by Staddon, J. "Another approach to inference control [3] is to determine at query time whether a query can be safely answered. This can be done, for example, by maintaining user query histories. When a user makes a query it is checked against the user's query history and all known inference channels, before granting access to the results of the query."
3. The article by Li Yang stated two more ways of auditing "The fifth category is to audit changes to sources of stored procedures and triggers where malicious codes can easily hide. The sixth

category is to audit database errors because attackers will make many attempts before they get it right."

Improvements:

Perhaps a good way to improve this study would be to examine the possibility of "unreported data breaches". Not every breach can be discovered, sometimes internal factors can make it difficult to track, and at other times, the hackers use advanced techniques that are fully undetectable. For example: if a database admin's computer is infected via a remote access trojan and his/her pc is used to access the database, then there are not many ways to track.

References:

1. Murray, M. C. (2010). Database security: What students need to know. Journal of information technology education: Innovations in practice, 9, IIP-61.

2. Yang, L., 2009. Teaching database security and auditing. Proceedings of the 40th ACM Technical Symposium on Computer Science Education, Chattanooga, TN, USA.

3. Staddon, J. (2003). Dynamic inference control. Proceedings of the 8th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery, San Diego, CA, USA, 94-100.