نام درس (فارسی)	امنیت پایگاه داده‌ها
نام درس (انگلیسی)	Database Security

شماره درس: ۴۰-۷۳۴	تعداد واحد: ۳	مقطع: تحصیلات تکمیلی
پیش‌نیازها: پایگاه داده ها (درس کارشناسی)		هم‌نیازها: -
تهیه‌کننده: رسول جلیلی		

هدف

این درس در برگیرنده نکات منطقی در رابطه با امنیت پایگاه داده‌ها است. از آنجا که مهم‌ترین مساله امنیتی در پایگاه داده‌ها، مساله کنترل دسترسی به داده‌ها می‌باشد، بخش عمده‌ای از مباحث درس به مدل‌های کنترل دسترسی (اختیاری، اجباری و نقش-مبنا) می‌پردازد. این مدل‌ها از ابعاد مختلف و با هدف حفظ محرمانگی و صحت داده‌ها در سیستم های پایگاه داده‌ها مرور گشته، و مدل سازی سیستم های پایگاه داده ها همراه با نکات پیاده سازی مانند تجزیه ناپذیری(atomicity)، پی در پی سازی (serialization)، و کنترل مبتنی بر دیدگاه (View) مطرح می شود. همچنین مسائلی مانند نشر پذیری (releasability) در طراحی پایگاه داده امن و انواع معماری‌های امن پایگاه‌داده‌ها مورد بررسی قرار می‌گیرند. مساله حفظ امنیت در پایگاه‌داده‌های غیر رابطه‌ای و نوین از جمله پایگاه داده‌های آماری، پایگاه داده‌های شی‌گرا، پایگاه‌داده‌های مبتنی بر مستندات XML و آنتولوژی از جمله مباحث دیگری است که در این درس بدان پرداخته می‌شود. هدف اصلی از طرح این بخش آشنایی با مسائلی همچون کانال‌های استنتاج و کنترل آنها و همچنین انتشار دسترسی‌ها بر اساس روابط ارث‌بری و روابط معنایی حاکم بر این محیط‌ها می‌باشد. در کنار مسائل فوق، به مواردی همچون جمع‌آوری و استفاده از پایگاه داده‌های بازرسی همراه با تشخیص نفوذ و کنترل دسترسی قیدی و الزامی نیز پرداخته می‌شود. در نهایت، مکانیزم‌های کنترل امنیت در پایگاه‌داده‌های اوراکل به طور نمونه مورد بررسی قرار می‌گیرند.

سرفصل مطالب

۱. مقدمه
   a. مقدمه ای بر پایگاه داده ها (مفاهیم یک پایگاه داده، اجزاء یک پایگاه داده، پرس و جو (query)،مزایای استفاده)
   b. خواسته های امنیتی (یکپارچگی پایگاه داده و صحت المان ها، قابلیت بازرسی، کنترل دستیابی، تصدیق اصالت کاربر، دسترسی پذیری، قابلیت اعتماد (reliability))
   c. اطلاعات حساس (عوامل حساس سازی، تصمیم های مختلف در مورد دسترسی، دسترس پذیری داده ها، اطمینان از اصالت، انواع افشاء شدن، امنیت و دقت)
۲. مدل‌های امنیتی
   a. کنترل دسترسی
   b. مسأله استنتاج و کانال های نهان
   c. خط‌مشی باز در مقابل بسته
   d. کنترل دسترسی اختیاری در مقابل اجباری
۳. مدل‌های کنترل دسترسی اختیاری
   a. مدل‌های ماتریس-مبنا عمومی
   b. مدل‌های گراف-مبنای عمومی
   c. مدل‌های کنترل دسترسی اختیاری خاص پایگاه‌داده‌ها

۴. مدل‌های کنترل دسترسی اجباری
   a. مدل‌های حفظ محرمانگی عمومی
   b. مدل‌های حفظ صحت عمومی
   c. مدل‌های کنترل دسترسی پایگاه‌داده‌های چند سطحی (از بُعد محرمانگی و صحت)
   d. معماری DBMS امن چند سطحی
۵. مدل‌های کنترل دسترسی نقش-مبنا و مدیریت آنها
   a. انواع مدل‌های نقش-مبنا
   b. مدل مدیریت کنترل دسترسی نقش- مبنا
۶. امنیت پایگاه داده‌های آماری
   a. تکنیک‌های مفهومی
   b. تکنیک‌های محدودساز
   c. تکنیک‌های تشویش‌گرا
۷. مدل‌های امنیتی نسل‌های بعدی پایگاه‌داده‌ها
   a. کنترل دسترسی در پایگاه‌داده‌های شیئ‌گرا
   b. کنترل دسترسی در پایگاه‌داده‌های مبتنی بر XML
   c. کنترل دسترسی در پایگاه‌داده‌های مبتنی بر آنتولوژی
۸. مدل‌های کنترل دسترسی قیدی و الزامی
۹. مکانیزم‌های بازرسی در پایگاه داده‌های رابطه‌ای
۱۰. معماری های امن پایگاه داده
۱۱. برونسپاری امن پایگاه داده ها
۱۲. مطالعه موردی (مکانیزم‌های امنیتی در نسخ مختلف Oracle)

منابع

1. S. Castano, M. G. Fugini, G. Martella, and P. Samarati, "Database Security," Addison-Wesley, 1996.
2. E. Bertino, R. Sandhu, "Database Security – Concepts, Approaches, and Challenges," IEEE Transaction on Dependable and Secure Computing, vol. 2, no. 1, 2005.

منابع کمکی درس

3. M. Bishop, Computer Security: Art and Science, 2nd ed: Addison-Wesley, 2003.
4. J. A. Goguen and J. Meseguer, "Security Policy and Security Models," presented at IEEE Symposium on Security and Privacy, 1982.
5. D. E. Denning, "Secure Distributed Data Views: The Sea-View Formal Security Model," SRI International, Technical Report A003, 1987.
6. K. P. Smith and M. S. Winslett, "Entity Modeling in the MLS Relational Model," presented at 18th Conference on Very Large Databases, Vancouver, Canada, 1992.
7. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," IEEE Computer, vol. 29, pp. 38-47, 1996.
8. M. Nyanchama and S. L. Osborn, "The Role Graph Model and Conflict of Interest," ACM Transaction on Information Systems Security, vol. 2, pp. 3-33, 1999.

9. R. S. Sandhu, V. Bhamidipati, E. J. Coyne, S. Ganta, and C. E. Youman, "The ARBAC97 Model for Role-Based Administration of Roles: Preliminary Description and Outline," presented at ACM Workshop on Role-Based Access Control, 1997.
10. D. E. Denning and J. Schlörer, "Inference Controls for Statistical Databases," *IEEE Computer*, vol. 16, pp. 69-82, 1983.
11. D. Denning Views for Multi-level Data base Security IEEE Trans- Software Eng. 1987.
12. E. Bertino and H. Weigand, "An Approach to Authorization Modeling in Object-Oriented Database Systems," Data and Knowledge Engineering, vol. 12, pp. 1-29, 1994.
13. A. Gabillon and E. Bruno, "Regulating Access to XML Documents," presented at 5th Annual Working Conference on Database and Application Security (DAS'01), Niagara, Ontario, Canada, 2002.
14. E. Damiani, S. D. C. d. Vimercati, S. Paraboschi, and P. Samarati, "Securing XML Documents," presented at International Conference on Extending Database Technology (EDBT 2000), Konstanz, Germany, 2000.
15. M. Kudo and S. Hada, "XML Document Security based on Provisional Authorization," *presented at ACM Conference on Computer and Communication Security (CCS 2000)*, 2000.
16. A. Masoumzadeh, M. Amini, and R. Jalili, "Context-Aware Provisional Access Control," *presented at 2nd International Conference on Information Systems Security (ICISS'06)*, Kolkata, India, 2006.
17. S. Javanmardi, M. Amini, and R. Jalili, "An Access Control Model for Protecting Semantic Web Resources," presented at 2nd International Semantic Web Policy Workshop (SWPW'06) 2006, Athens, GA, USA, 2006.
18. M. Theriault and A. Newman “Oracle Security Handbook” Osbornc/McGraw-Hill 2001

نحوه ارزیابی:

- تمرین — حداقل ٪۱۰
- امتحان میان نیمسال — حداقل ٪۲۰
- امتحان پایان نیمسال — حداقل ٪۳۰
- مقاله مروری درس وارائه در روز سمینار — حداقل ٪۱۵