CS 3002 Information Security

Fall 2023

1. Explain key concepts of information security such as design principles, cryptography, risk management,(1)

2. Discuss legal, ethical, and professional issues in information security (6)
3. Analyze real world scenarios, model them using security measures, and apply various security and risk management tools for achieving information security and privacy (2)
4. Identify appropriate techniques to tackle and solve problems of real life in the discipline of information security (3)
5. Understand issues related to ethics in the field of information security(8)

ISO/IEC 27001: 2013

Week # 8

Dr. Nadeem Kafi Khan

Coverage in Week # 8

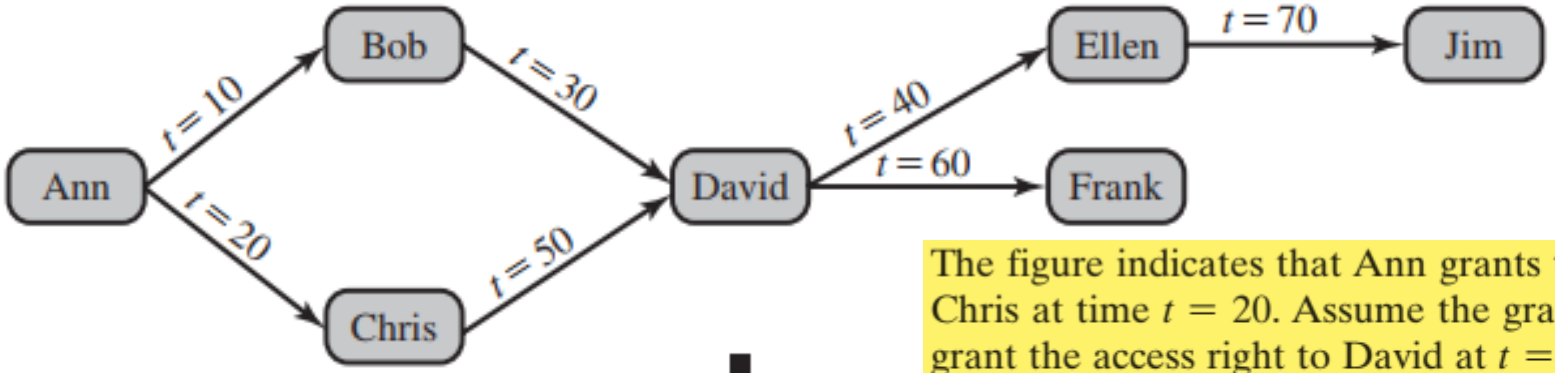
- Topics coverage after Midterm # 1 (see attached snap)
- SQL Injection (SQLi) Attack – Introduction
- How to limit SQLi risk using RBAC?
- How to setup a RBAC for an application schema? (see attached snap)
- Cascading Authorizations
- Inference and Inference example
- Friday 13th Oct Class
  - Quiz # 2
  - Assignment # 1 hardcopy submission assessment

Self Study

CHAPTER 5

DATABASE AND DATA CENTER SECURITY

Cascading Authorizations



The figure indicates that Ann grants the access right to Bob at time $t = 10$ and to Chris at time $t = 20$. Assume the grant option is always used. Thus, Bob is able to grant the access right to David at $t = 30$. Chris redundantly grants the access right to David at $t = 50$. Meanwhile, David grants the right to Ellen, who in turn grants it to Jim; and subsequently David grants the right to Frank.

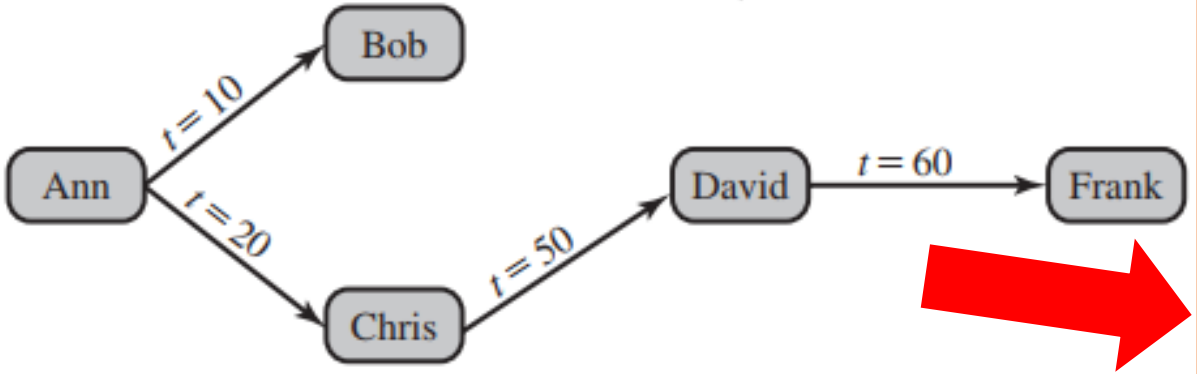


Figure 5.6 **Bob Revokes Privilege from David**

- Suppose Bob revokes the privilege from David. David still has the access right because it was granted by Chris at $t = 50$.
- The access rights to Ellen and Jim is revoked when Bob revokes the access right to David.
- **Why?** This is because at $t = 40$, when David granted the access right to Ellen, David only had the grant option to do this from Bob. When Bob revokes the right, this causes all subsequent cascaded grants that are traceable solely to Bob via David to be revoked.

5.6 INFERENCE

- Inference, as it relates to database security, is the process of performing authorized queries and deducing unauthorized information from the legitimate responses received.
- The inference problem arises when the combination of a number of data items is more sensitive than the individual items, or when a combination of data items can be used to infer data of higher sensitivity.
- Figure 5.7 illustrates the process. The attacker may make use of non sensitive data as well as metadata. The information transfer path by which unauthorized data is obtained is referred to as an **inference channel**.
- Two inference techniques can be used to derive additional information:
  - Analyzing functional dependencies between attributes within a table or across tables, and
  - Merging views with the same constraints.

Metadata refers to knowledge about correlations or dependencies among data items that can be used to deduce information not otherwise available to a particular user.

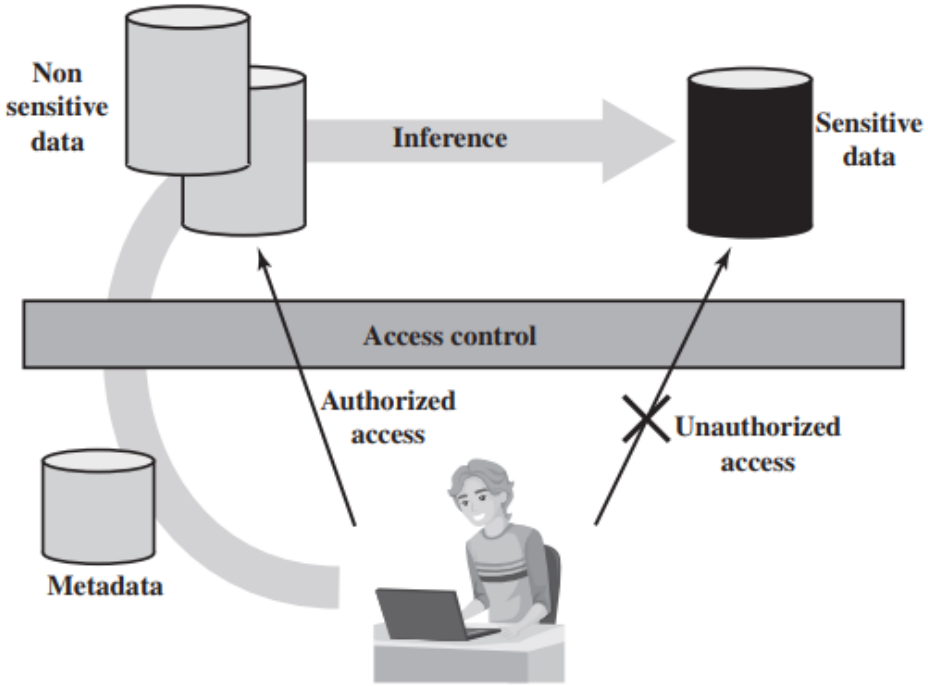


Figure 5.7 **Indirect Information Access via Inference Channel**

5.6 INFERENCE

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware
Cake pan	online only	12.99	housewares
Shower/tub cleaner	in-store/online	11.99	housewares
Rolling pin	in-store/online	10.99	housewares

(a) Inventory table

```
CREATE view V1 AS
SELECT Availability, Cost
FROM Inventory
WHERE Department = "hardware"
```

```
CREATE view V2 AS
SELECT Item, Department
FROM Inventory
WHERE Department = "hardware"
```

Availability	Cost ($)
in-store/online	7.99
online only	5.49
in-store/online	104.99

Item	Department
Shelf support	hardware
Lid support	hardware
Decorative chain	hardware

(b) Two views

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware

(c) Table derived from combining query answers

Figure 5.8 Inference Example

A user who knows the structure of the Inventory table and who knows that the view tables maintain the same row order as the Inventory table is then able to merge the two views to construct the table shown in Figure 5.8c. This violates the access control policy that the relationship of attributes Item and Cost must not be disclosed.