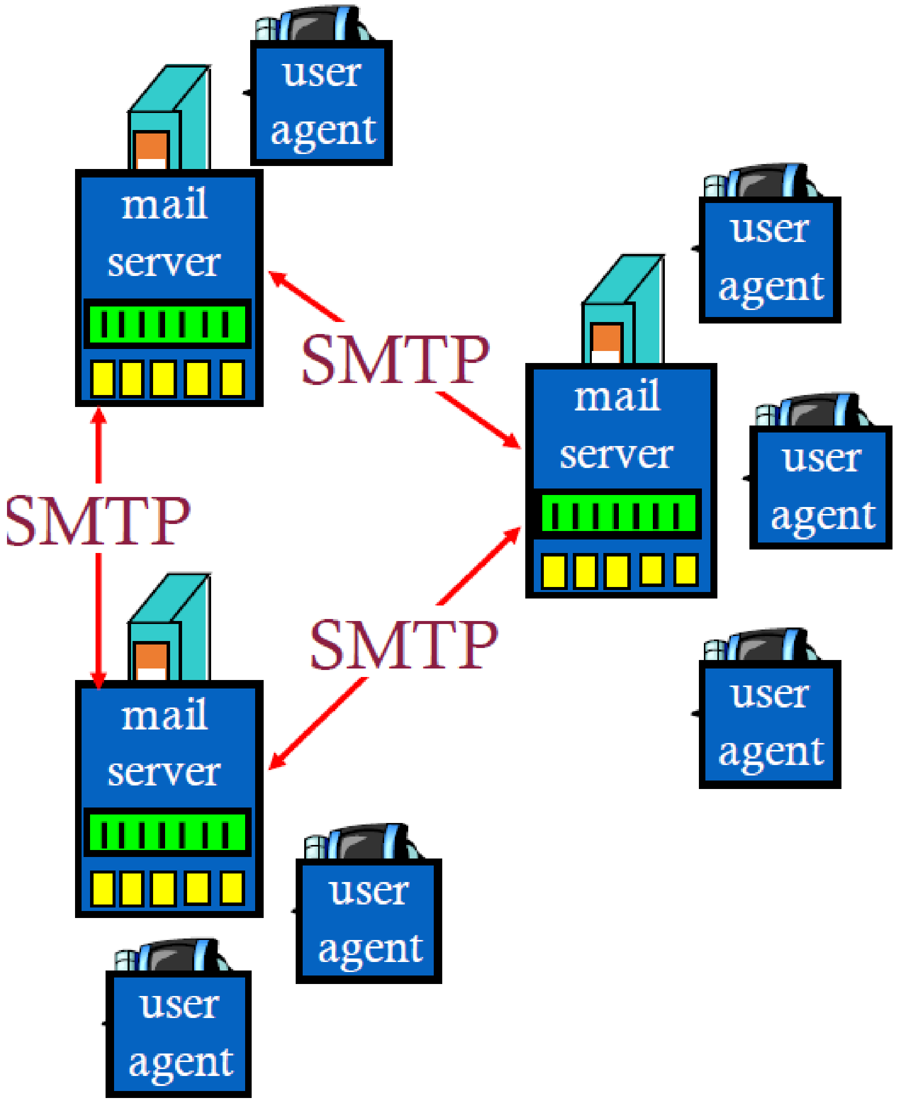
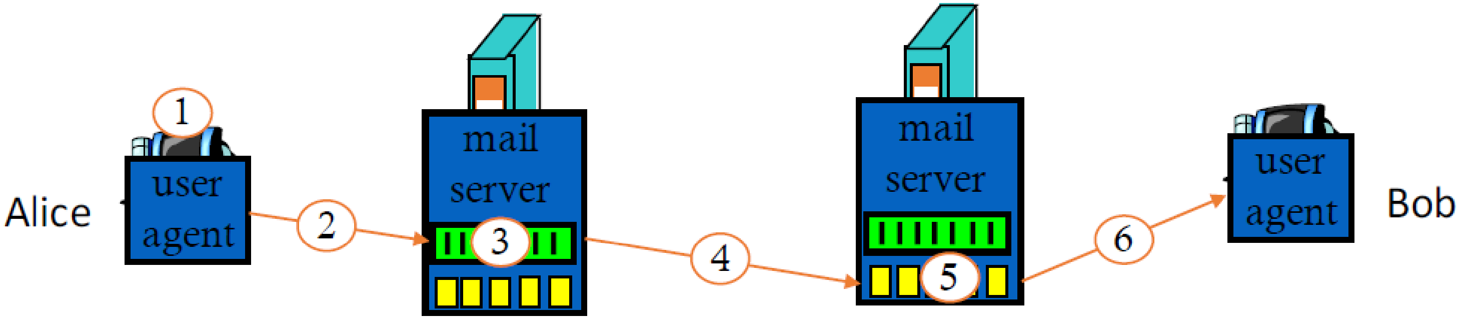
Email basics

- Three major components:
  - user agents, mail servers, transfer protocol: SMTP
- User agent
  - a.k.a. “mail reader”, e.g., outlook
  - composing, editing, reading mail messages
- Mail Servers
  - Mailbox contains incoming mails for user
  - And message queue of outgoing mails
- SMTP protocol
  - Mail servers to send email messages



Email: SMTP

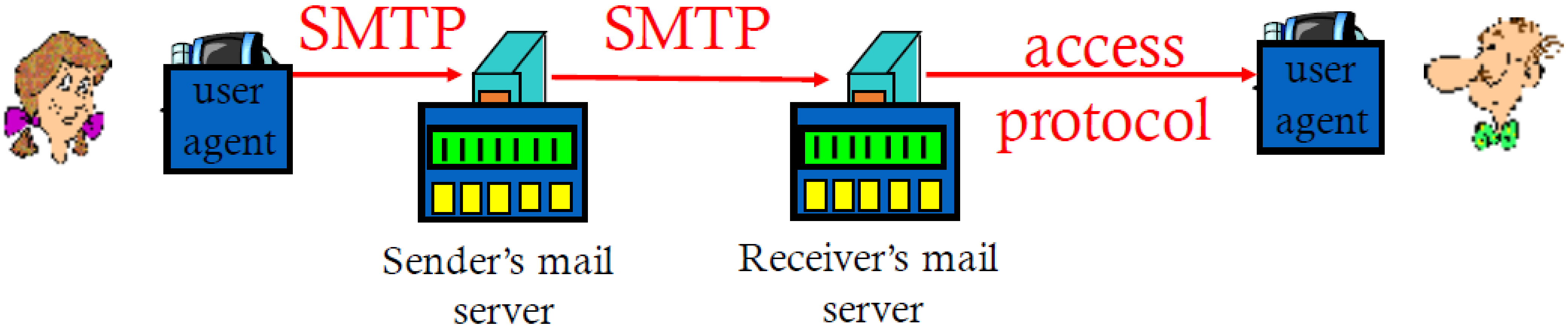
- Uses TCP to reliably transfer email message using Port 25
- Scenario: Alice sends message to Bob
  - 1) Alice uses UA to compose message and “to” bob@hamburger.edu
  - 2) Alice’s UA sends message to her mail server (e.g. crepes.fr); msg placed in message queue
  - 3) Client side of SMTP opens TCP connection with Bob’s mail server
  - 4) SMTP client sends Alice’s message over the TCP connection
  - 5) Bob’s mail server places the message in Bob’s mailbox
  - 6) Bob invokes his user agent to read message (access protocols)



Sample SMTP interaction

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250  Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

Mail access protocols



- Mail access protocol: retrieval from server
  - POP: Post Office Protocol [RFC 1939]: authorization (agent <-->server) and download
  - IMAP: Internet Mail Access Protocol [RFC 1730]: more features (more complex)
  - HTTP(s): gmail, Hotmail, Yahoo! Mail, etc.

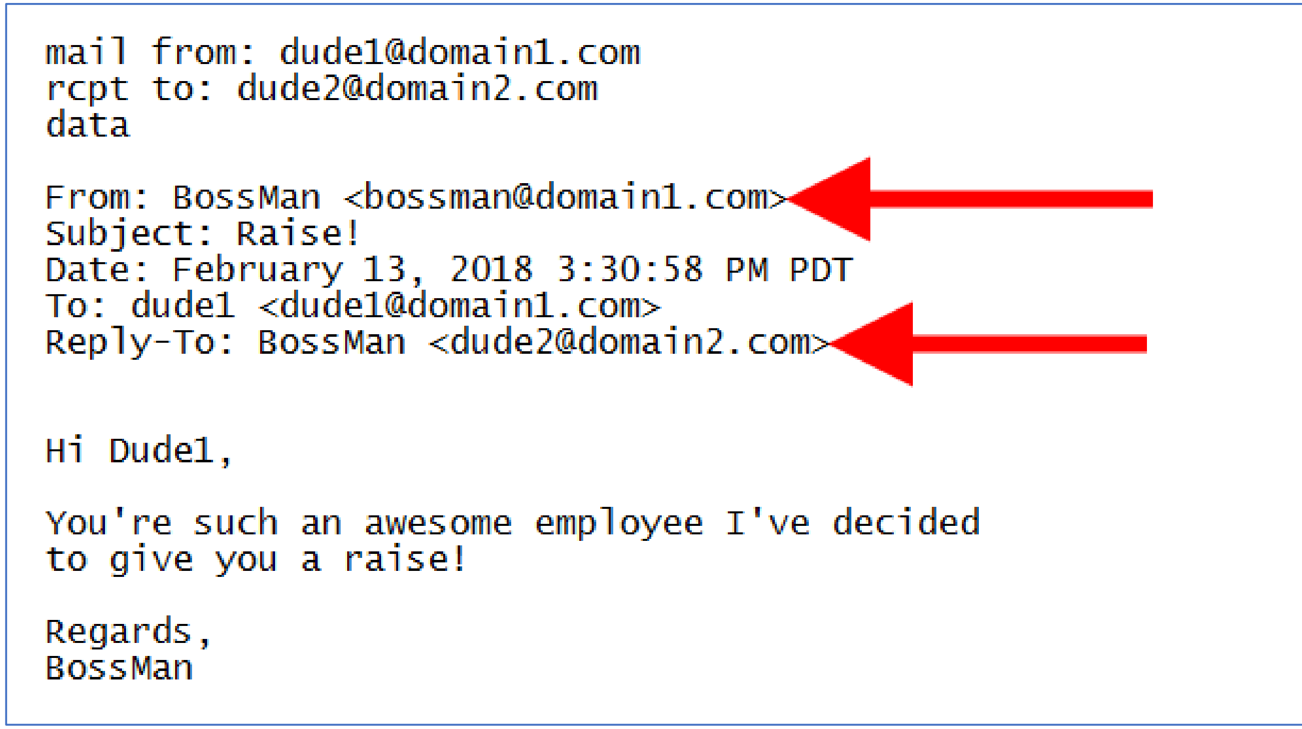
Email Spoofing

- SMTP has no authentication & verification
  - "MAIL FROM" (also called Return-Path, the delivery address of the reply email, invisible to user) can be set to anything (e.g., a spoofing target)
  - "From" fields (directly visible to users) in mail header can be changed to anything
  - "MAIL FROM" and "From" can be entirely different

- Widely used for spear phishing

Example of Email Spoofing

- Prank from your colleague
- “Mail from” is the real address
- “From” is your boss (faked)
- “RCPT to” is the real receiver
- “Reply to” is your boss (faked)



```
mail from: dude1@domain1.com
rcpt to: dude2@domain2.com
data

From: BossMan <bossman@domain1.com>
Subject: Raise!
Date: February 13, 2018 3:30:58 PM PDT
To: dude1 <dude1@domain1.com>
Reply-To: BossMan <dude2@domain2.com>


Hi Dude1,

You're such an awesome employee I've decided
to give you a raise!

Regards,
BossMan
```

Countermeasures

- Authentication
  - SPF, DKIM and DMARC
- Confidentiality
  - PGP and S/MIME

- User education
  - Sender identity verification (check security indicators)
  - Online training (e.g., bait email)

Anti-spoofing Protocols

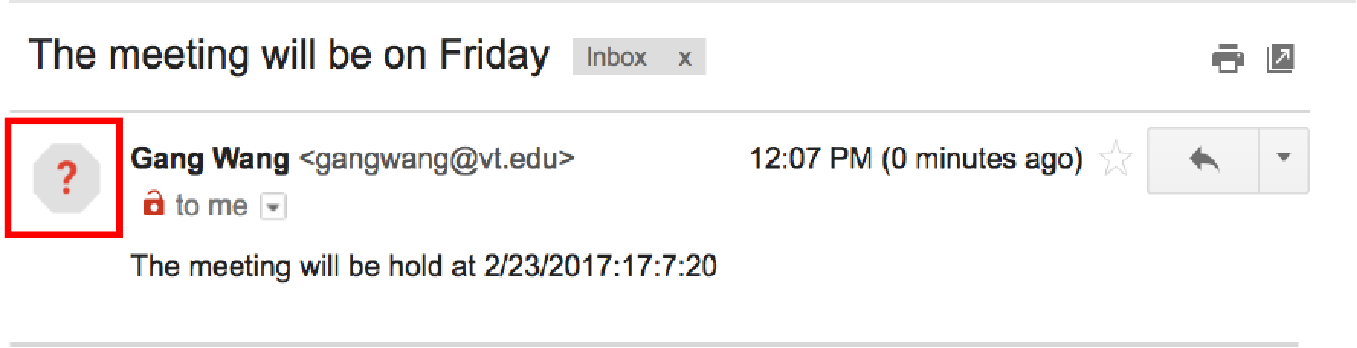
- Exist, but not widely adopted
- **SPF**: authentication by IP
  - DNS: specifies the IP range that can send email on behalf of x.com
- **DKIM**: public key based method
  - Sender domain signs the email
- **DMARC**:
  - Complementary to SPF and DKIM
  - Allows authentic senders to instruct email providers on how to handle unauthenticated mail via a DMARC policy, like quarantine, reject

PGP and S/MIME

- **PGP (Pretty Good Privacy)**
  - Use public key cryptography to sign, encrypt and decrypt emails
  - Session key (symmetric) for message encryption
  - Session key encrypted under recipient’s public key
  - Message digest signed by sender’s private key
  - PGP public keys are usually included at bottom of email or personal website
- **S/MIME**
  - Secure email attachments
  - S/MIME uses hierarchically validated certificates for key exchange
  - PGP depends on each user’s exchanging keys with recipients

Security indicators

- UI features
- Educating user to look for alarms
- Ignore and reject the messages failing the security checks

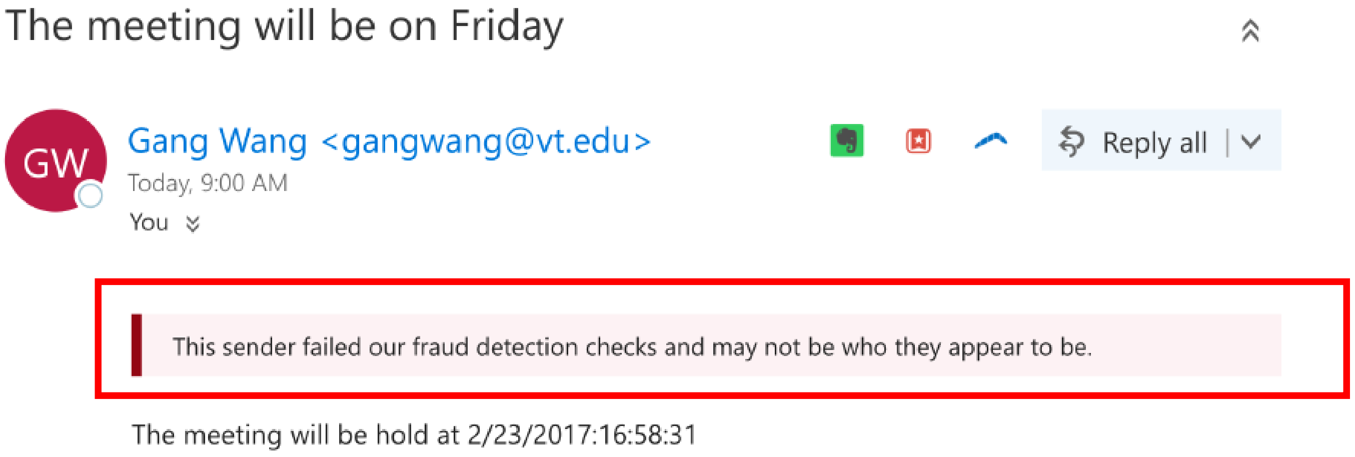


The meeting will be on Friday

Gang Wang <gangwang@vt.edu> 12:07 PM (0 minutes ago)

to me

The meeting will be hold at 2/23/2017:17:7:20



The meeting will be on Friday

Gang Wang <gangwang@vt.edu>

Today, 9:00 AM

You

This sender failed our fraud detection checks and may not be who they appear to be.

The meeting will be hold at 2/23/2017:16:58:31

Summary

- As web browsers have become a primary focus of users and taken on greater functionality, they’ve become a focus of many types of attack
- Browser and website weaknesses are often the result of some form of poor authentication
- Many attackers focus on tricking users with fake websites, misleading applications, and phishing emails
- Injection attacks (XSS, XSRF) are a key concern, and countermeasures to prevent them are critical
- Spam consists of large email volume, and email spoofing is a practical threat

Slides credit

- Security in computing 5th edition, Textbook Slides
- Web security, Gang Wang
- Web application security, John Mitchell

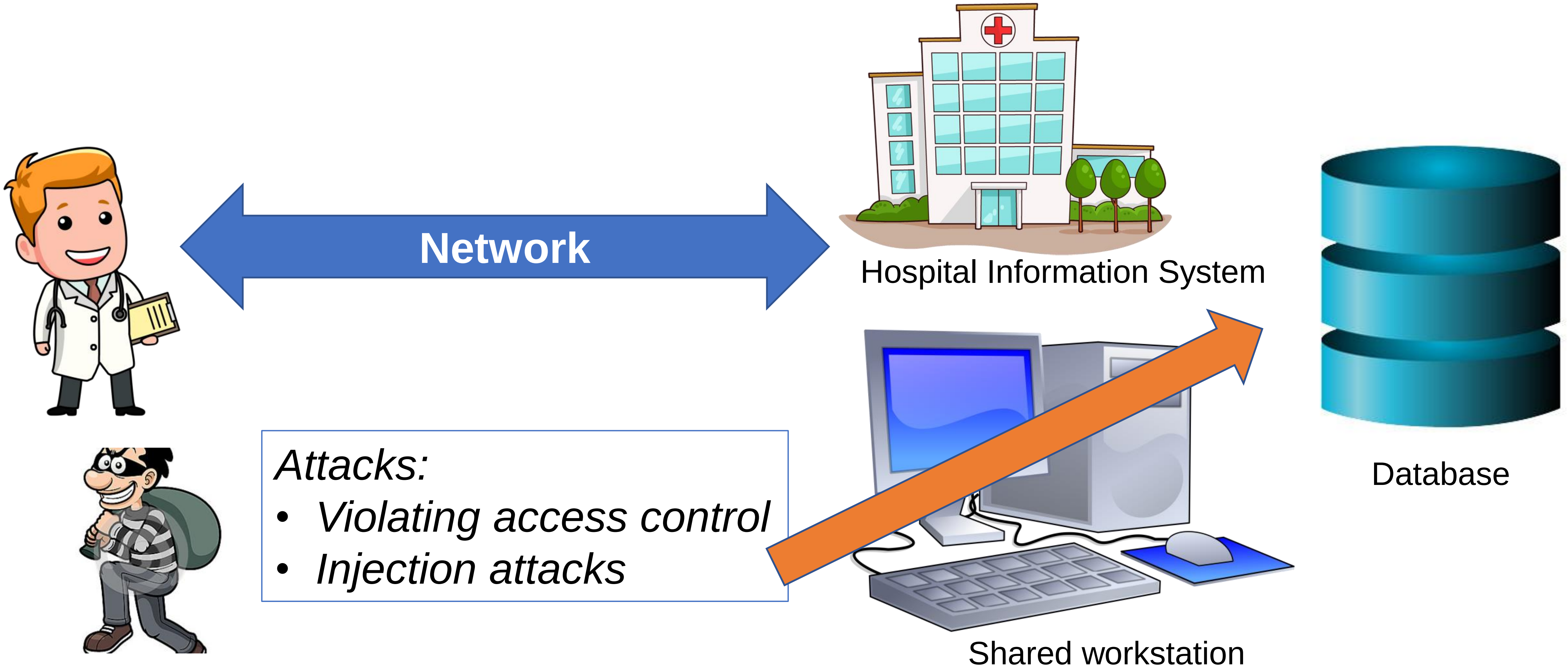
Databases

EECS 195

Spring 2019

Zhou Li

Security issues with Database



Attacks:

- *Violating access control*
- *Injection attacks*

Objectives

- Basic database terminology and concepts
- Security requirements for databases
- Implementing access controls in databases
- Protecting sensitive data
- Data mining and big data
- SQL Injection

Database Quick Overview

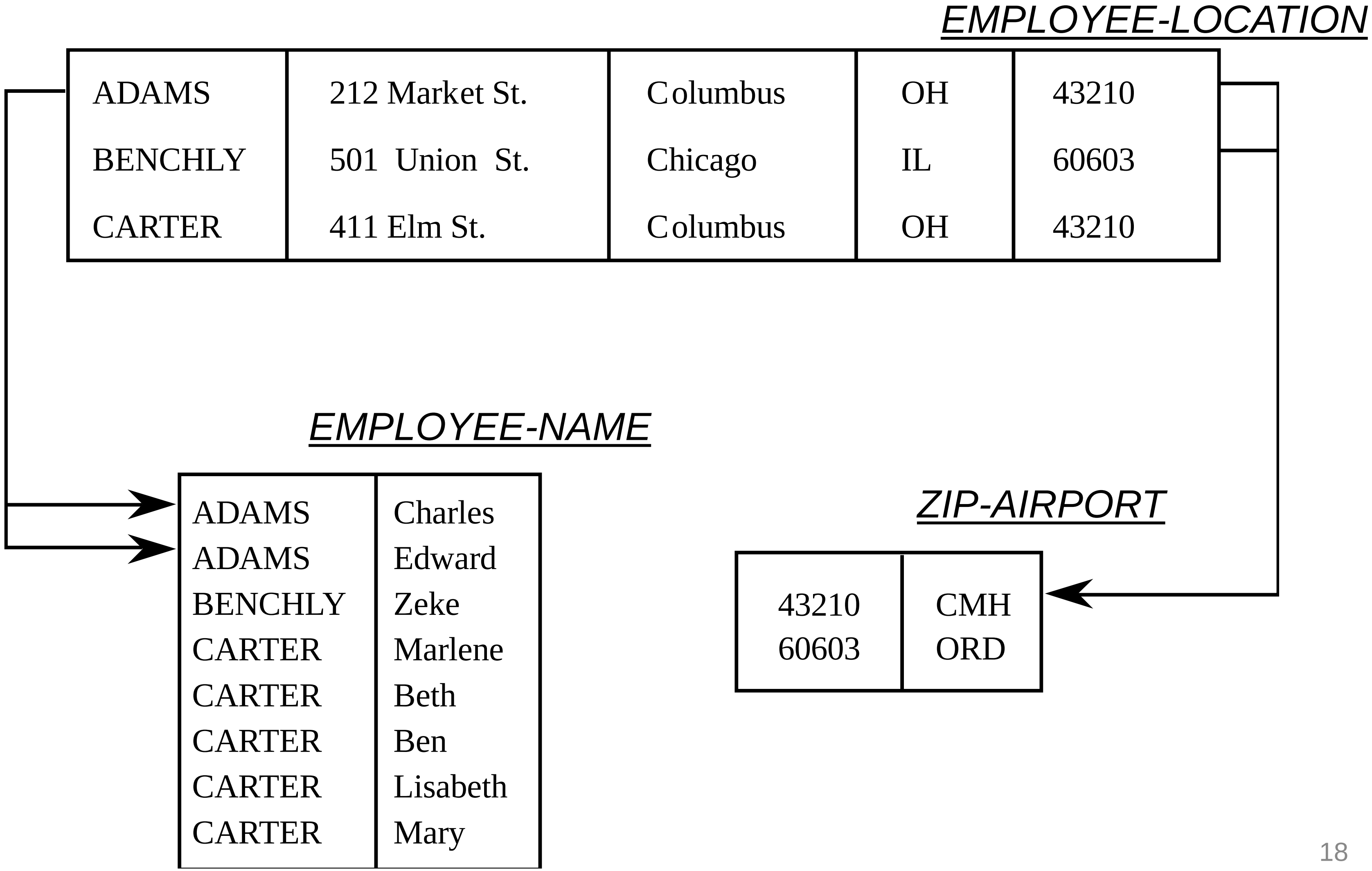
- Database
  - A collection of data and a set of rules of relationships among the data
- Database management system (DBMS)
  - The system through which users interact with the database
  - E.g., Oracle, MS SQL Server, MySQL
- Record
  - One related group of data
- Field/element
  - Elementary data items that make up a record (e.g., name, address, city)

Database Quick Overview (cond.)

- Schema
  - Logical structure of a database
- Subschema
  - The portion of a database a given user has access to
- Attribute
  - A column in a database
- Relation
  - A set of database columns
  - Also connection among data across tables

Example of Database

- A database with three tables
- Use subschemas to present to users only the elements they wish or need to see.



EMPLOYEE-LOCATION

ADAMS	212 Market St.	Columbus	OH	43210
BENCHLY	501 Union St.	Chicago	IL	60603
CARTER	411 Elm St.	Columbus	OH	43210

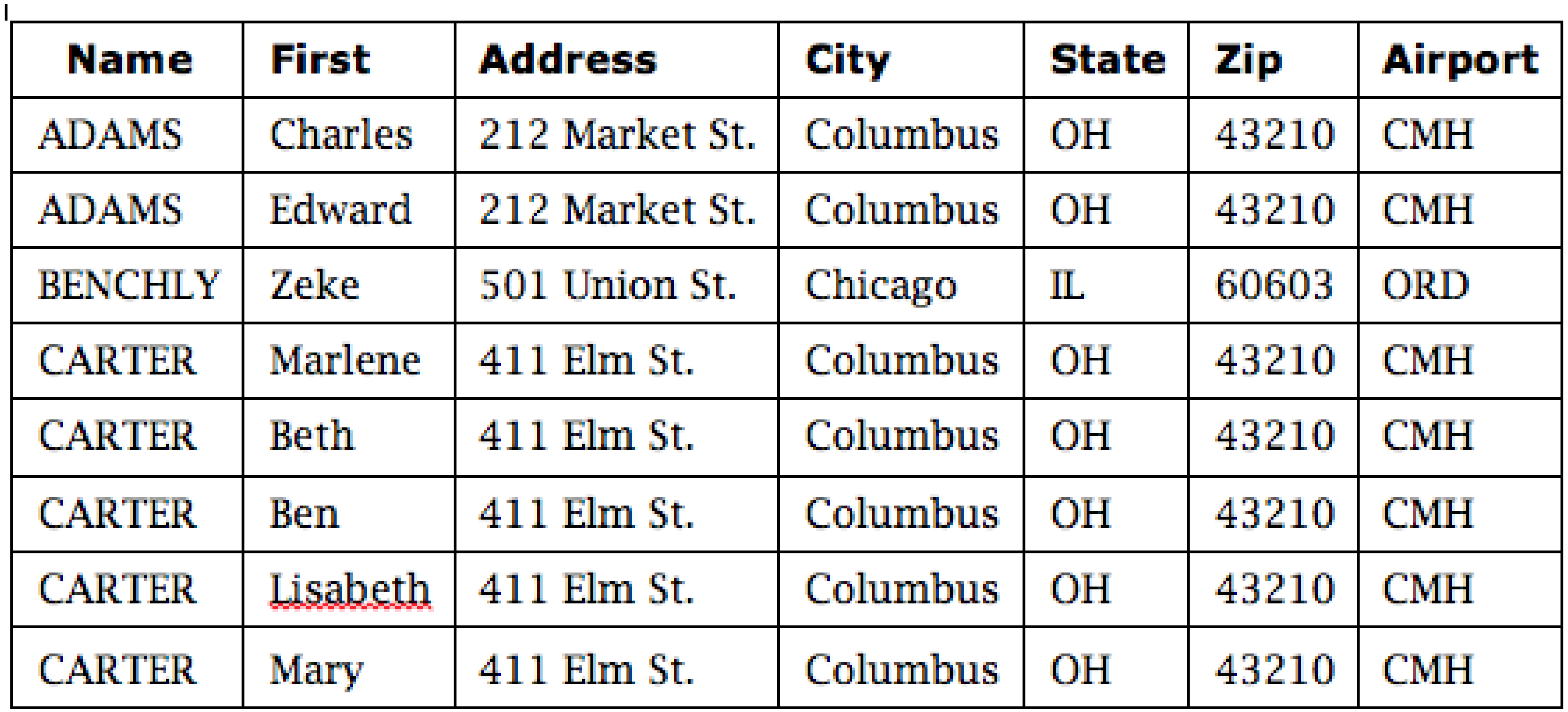
EMPLOYEE-NAME

ADAMS	Charles
ADAMS	Edward
BENCHLY	Zeke
CARTER	Marlene
CARTER	Beth
CARTER	Ben
CARTER	Lisabeth
CARTER	Mary

ZIP-AIRPORT

43210	CMH
60603	ORD

Overall Schema



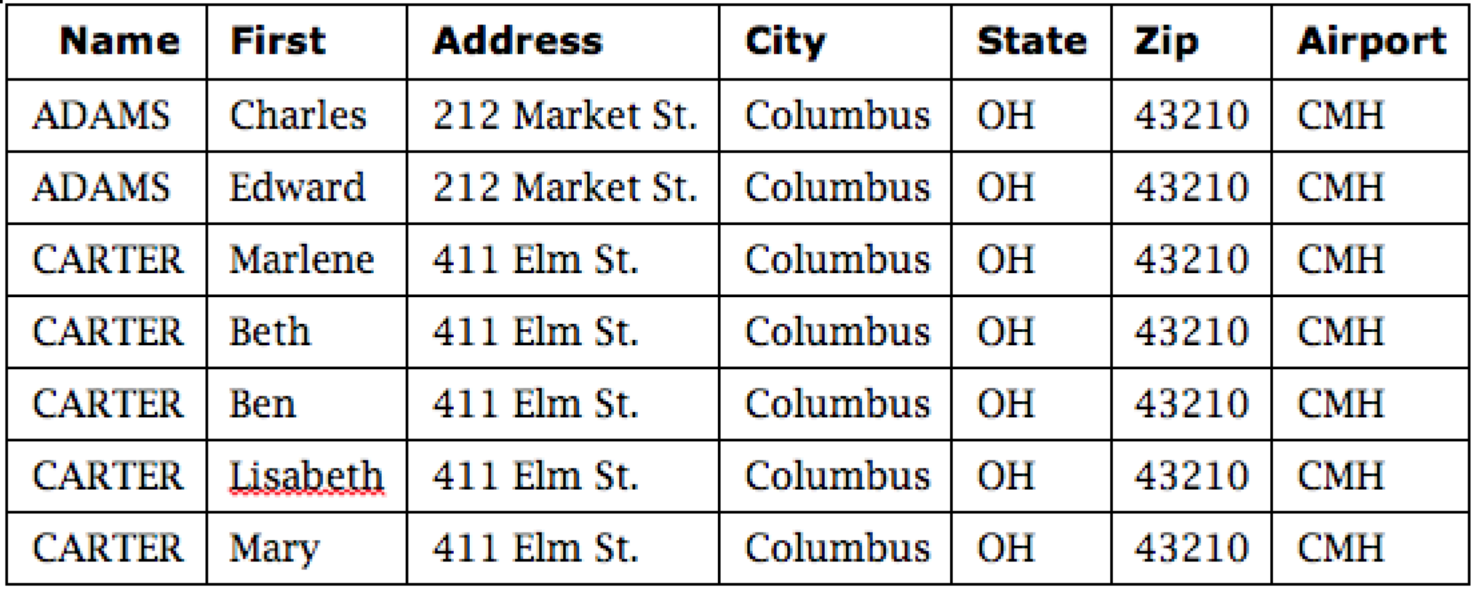
Name	First	Address	City	State	Zip	Airport
ADAMS	Charles	212 Market St.	Columbus	OH	43210	CMH
ADAMS	Edward	212 Market St.	Columbus	OH	43210	CMH
BENCHLY	Zeke	501 Union St.	Chicago	IL	60603	ORD
CARTER	Marlene	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Beth	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Ben	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Lisabeth	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Mary	411 Elm St.	Columbus	OH	43210	CMH

Queries

- A query is a command that tells the database to retrieve, modify, add, or delete a field or record
- The most common database query language is SQL
    - A structured language developed by IBM

Example SQL Query

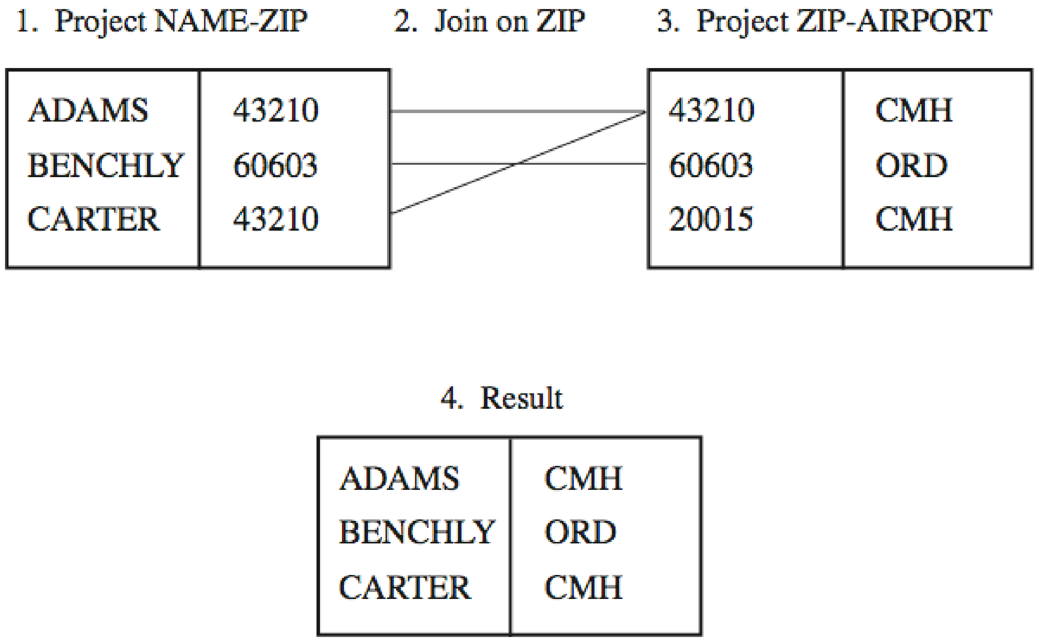
- SELECT ZIP=‘43210’ FROM SCHEMA



Name	First	Address	City	State	Zip	Airport
ADAMS	Charles	212 Market St.	Columbus	OH	43210	CMH
ADAMS	Edward	212 Market St.	Columbus	OH	43210	CMH
CARTER	Marlene	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Beth	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Ben	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Lisabeth	411 Elm St.	Columbus	OH	43210	CMH
CARTER	Mary	411 Elm St.	Columbus	OH	43210	CMH

Example SQL Query (cond.)

- Join query
- SELECT A.NAME, B.AIRPORT FROM NAME-ZIP AS A and ZIP-AIRPORT AS B WHERE A.ZIP=B.ZIP



1. Project NAME-ZIP

ADAMS	43210
BENCHLY	60603
CARTER	43210

2. Join on ZIP

3. Project ZIP-AIRPORT

43210	CMH
60603	ORD
20015	CMH

4. Result

ADAMS	CMH
BENCHLY	ORD
CARTER	CMH

Database Security Requirements

- Physical integrity
  - Immune from physical problems, like power failures
- Logical integrity
  - Modification of one field doesn’t affect other fields
- Element integrity
  - Data contained in each element are accurate
- Auditability
  - Can track who or what has accessed the elements

Database Security Requirements (cond.)

- Access control
  - A user is allowed to access only authorized data
  - Different users can be restricted to different modes of access
- User authentication
  - Every user is identified for accessing certain data
- Availability
  - Users can access the database in general and all the data for which they are authorized

Two-Phase Update

- Ensure the integrity of data modification
- Phase 1: Intent
  - DBMS does everything it can, other than making changes to the database, to prepare for the update
    - Collects records, opens files, locks out users, makes calculations
  - DBMS commits by writing a commit flag to the database
- Phase 2: Write
  - DBMS completes all write operations
  - DBMS removes the commit flag
- If the DBMS fails during either phase 1 or phase 2, it can be restarted and repeat that phase without causing harm