Infinite Connection

Build secure and reliable online services for MIT alumni

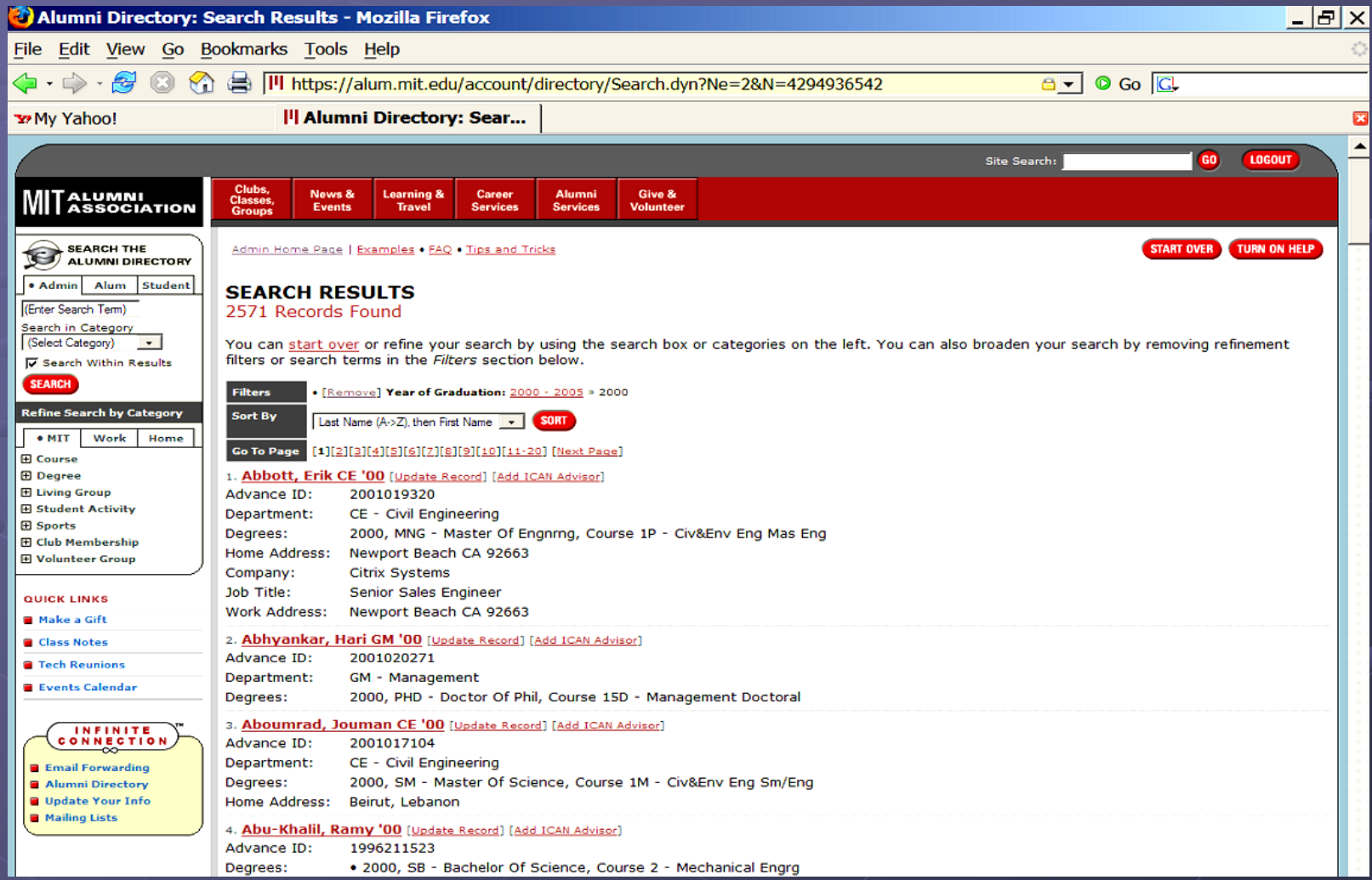
What is Infinite Connection?

- A collection of online services provided for MIT Alumni Community (alum.mit.edu)
- 2,000+ web pages
- 70,000+ registered alumni
- 1,200+ mailing lists to join
- 600,000+ searches on Online Alumni Directory annually

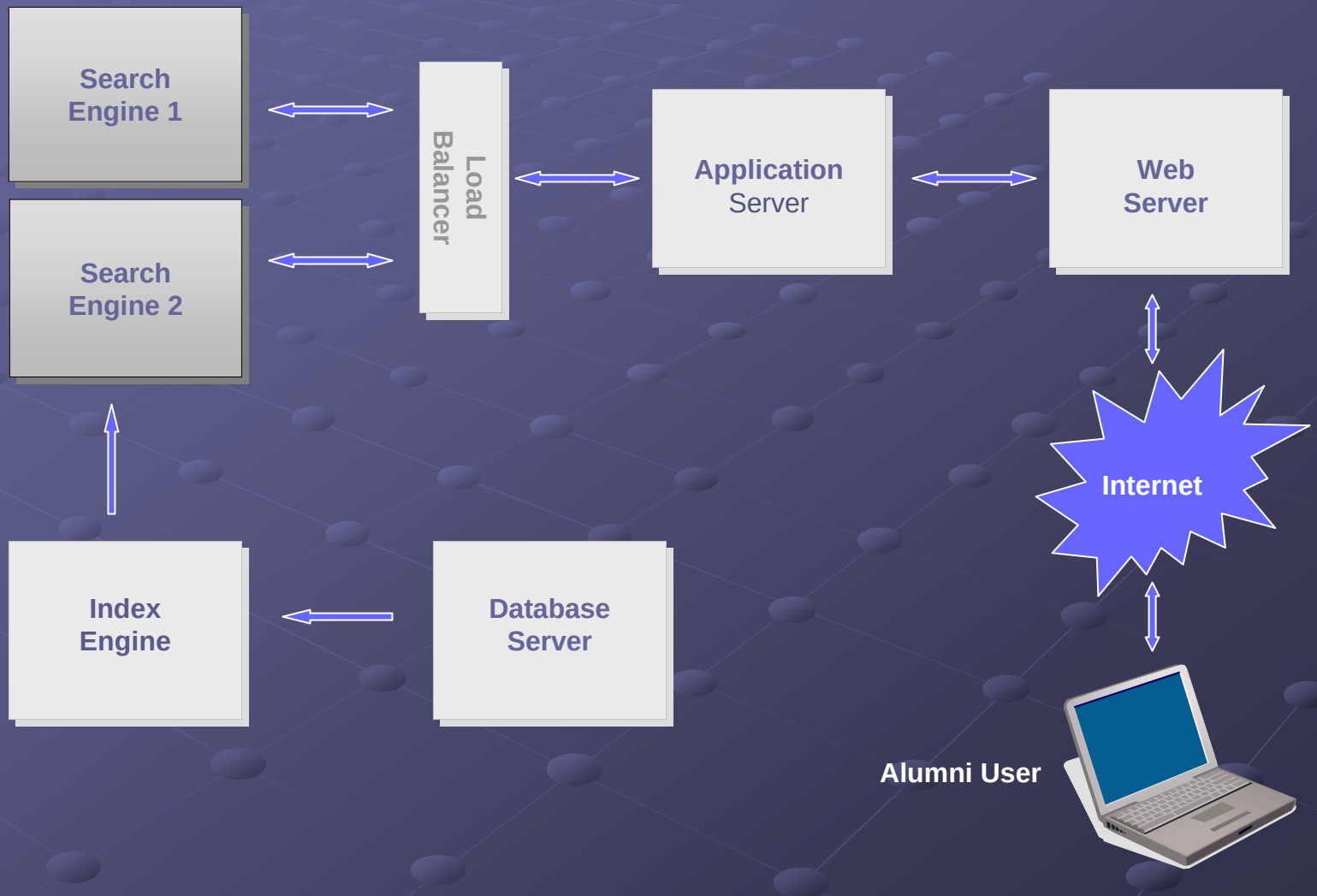
Services in Infinite Connection

- OAD (Online Alumni Directory)
- EFL (Email Forwarding for Life)
- SmarTrans (Online Event Registration and Club Dues Payment System)
- Mailing Lists, Online Elections, Job Posting, Online Class Notes
- and many many more …

Online Alumni Directory



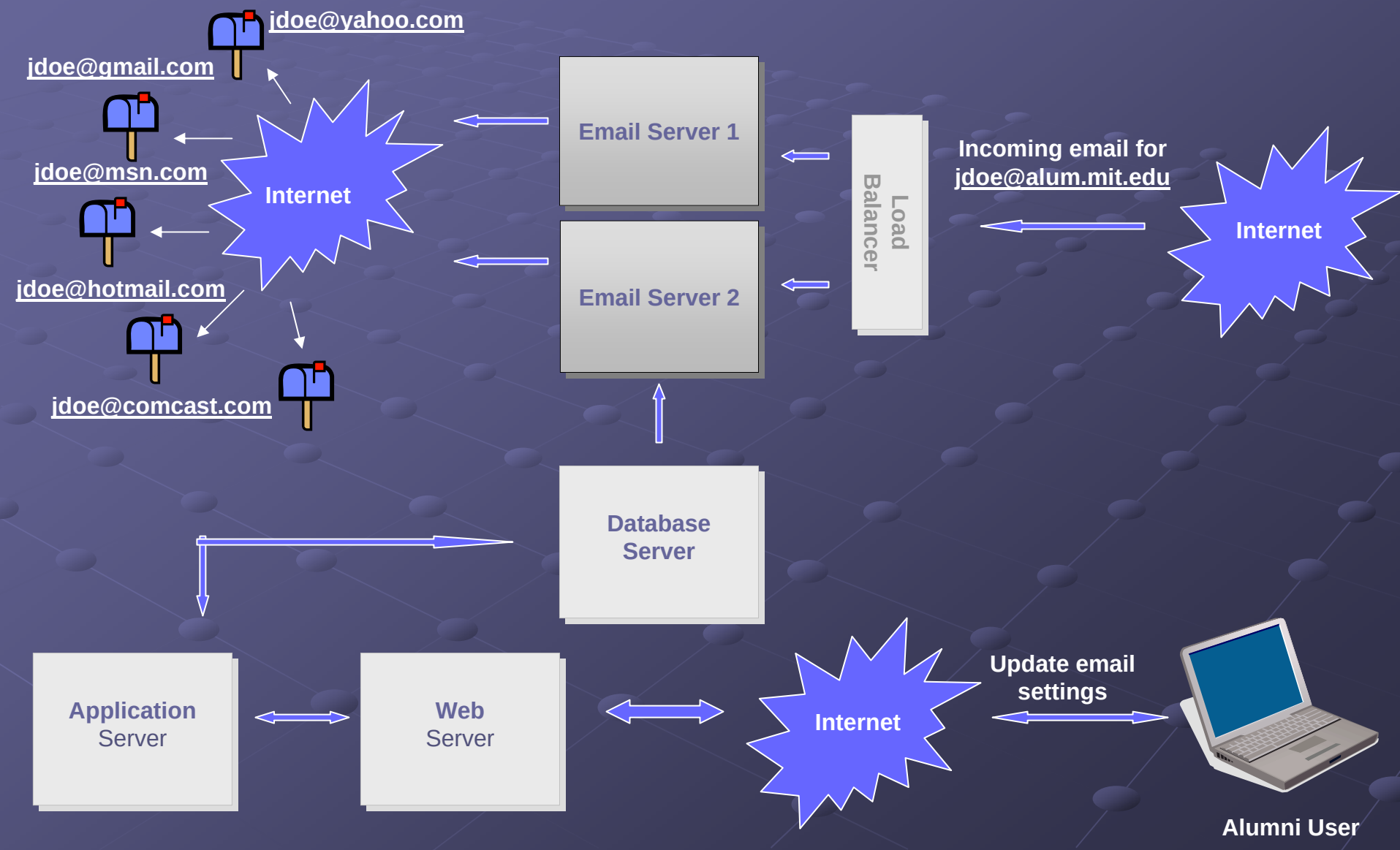
Online Alumni Directory



Email Forwarding for Life

- Life long email address: johndoe@alum.mit.edu
- Up to 5 forwarding email addresses
- Spam Filter, Allow List, Deny List
- Send email using @alum.mit.edu address from web
- Send email using @alum.mit.edu address from outgoing-alum.mit.edu server

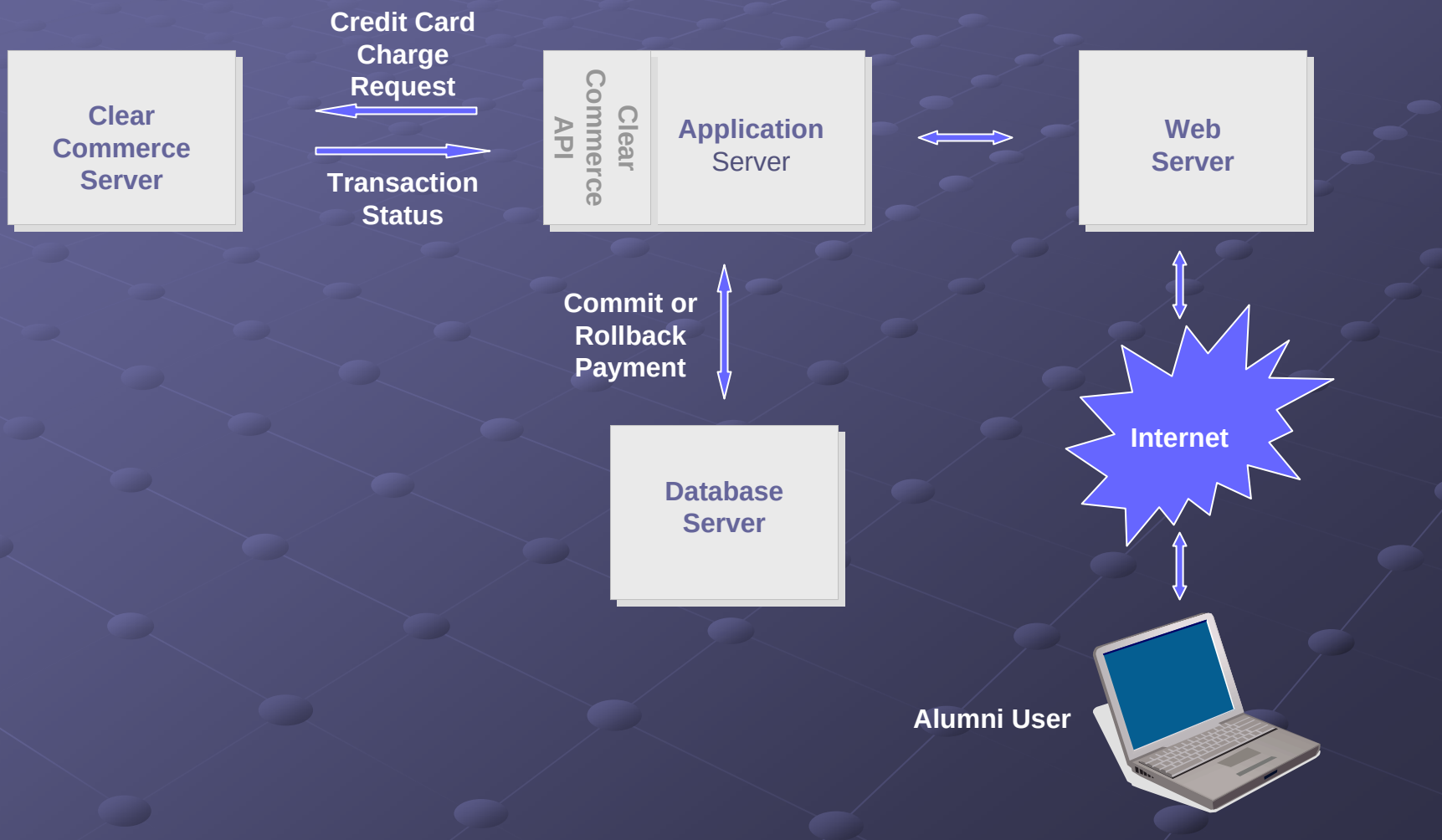
Email Forwarding for Life



SmarTrans

- Online Event Creation
- Online Event Registration
- Online Club Dues Payment
- 99 Clubs and Groups signed up
- 669 Events in 2005
- $548,221 online transactions in 2005

SmarTrans

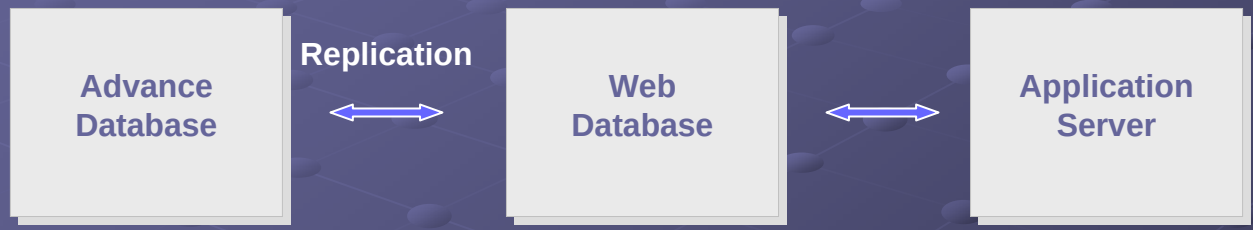

Credit Card Charge Request
Transaction Status
Clear Commerce Server
Clear Commerce API
Application Server
Web Server
Commit or Rollback Payment
Database Server
Internet
Alumni User

Security Matters

- March 2005 BC (120,000 alumni)
- March 2005 UC Berkeley (98,000 students)
- April 2005 Tufts (106,000 alumni)
- June 2006 UConn (72,000 students/faculty)
- April 2006 UTaxas (197,000 records)
- May 2006 VA (26.5 million veterans)

Design with Security in mind

- Database Design: Decouple advance and web database



- Access Policy: 37 different roles map to different access privileges
- Password Policy: at least 6 characters long, alphanumeric

Security Review

- We hired Symantec to perform a security review of our web application in 2005
- Some of the findings:
  - Weak Password: mit123, abc123, password1
  - SQL Injection
  - Input Validation: Cross Site Scripting (XSS)
  - Verbose Error Message

Security Review

- SQL Injection Case

```
PreparedStatement stmt=conn.prepareStatement(
        “select * from user_table where username =‘ ” +
        uname +  “’ and password = ‘ ” + pword + “ ’ ”);
ResultSet rs = stmt.executeQuery();
```

* uname = “johndoe’; -- ”

Security Review

- SQL Injection Defense: Bind Variables

```
PreparedStatement stmt=conn.prepareStatement(
        “select * from user_table where username = ? ” +
        “and password = ? ”);
stmt.setString(1, uname);
stmt.setString(2, pword);
ResultSet rs = stmt.executeQuery();
```

Security Review

- Cross Site Scripting

```
<table>
<tr>
  <td>Comments:</td>
  <td>$comments</td>
</tr>
</table>
```

* $comments = <script>alert(document.cookie);</script>

Security Review

- Cross Site Scripting Defense: Input Validation (HTML Escaping)

```
<table>
<tr>
  <td>Comments:</td>
  <td>#escapeHTML($comments)</td>
</tr>
</table>
```

* $comments = <script>alert(document.cookie);</script>

Latest Saga

- Our OAD activity log showed an alum accessed 35,000 alumni records in April 2006
- We implemented a daily query quota to prevent such incidents in the future
- Moral of the Lesson:
  - Log activity as much as possible
  - Give info as little as possible
  - Security is an ongoing battle

Q & A