

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

The screenshot shows a Mozilla Firefox browser window displaying the MIT Alumni Directory search results. The browser's address bar shows the URL: <https://alum.mit.edu/account/directory/Search.dyn?Ne=2&N=4294936542>. The page title is "Alumni Directory: Search Results - Mozilla Firefox".

The website header includes the MIT Alumni Association logo and navigation tabs for "Clubs, Classes, Groups", "News & Events", "Learning & Travel", "Career Services", "Alumni Services", and "Give & Volunteer". A search bar with "GO" and "LOGOUT" buttons is located in the top right corner.

The main content area displays "SEARCH RESULTS" with "2571 Records Found". Below this, a message states: "You can [start over](#) or refine your search by using the search box or categories on the left. You can also broaden your search by removing refinement filters or search terms in the *Filters* section below."

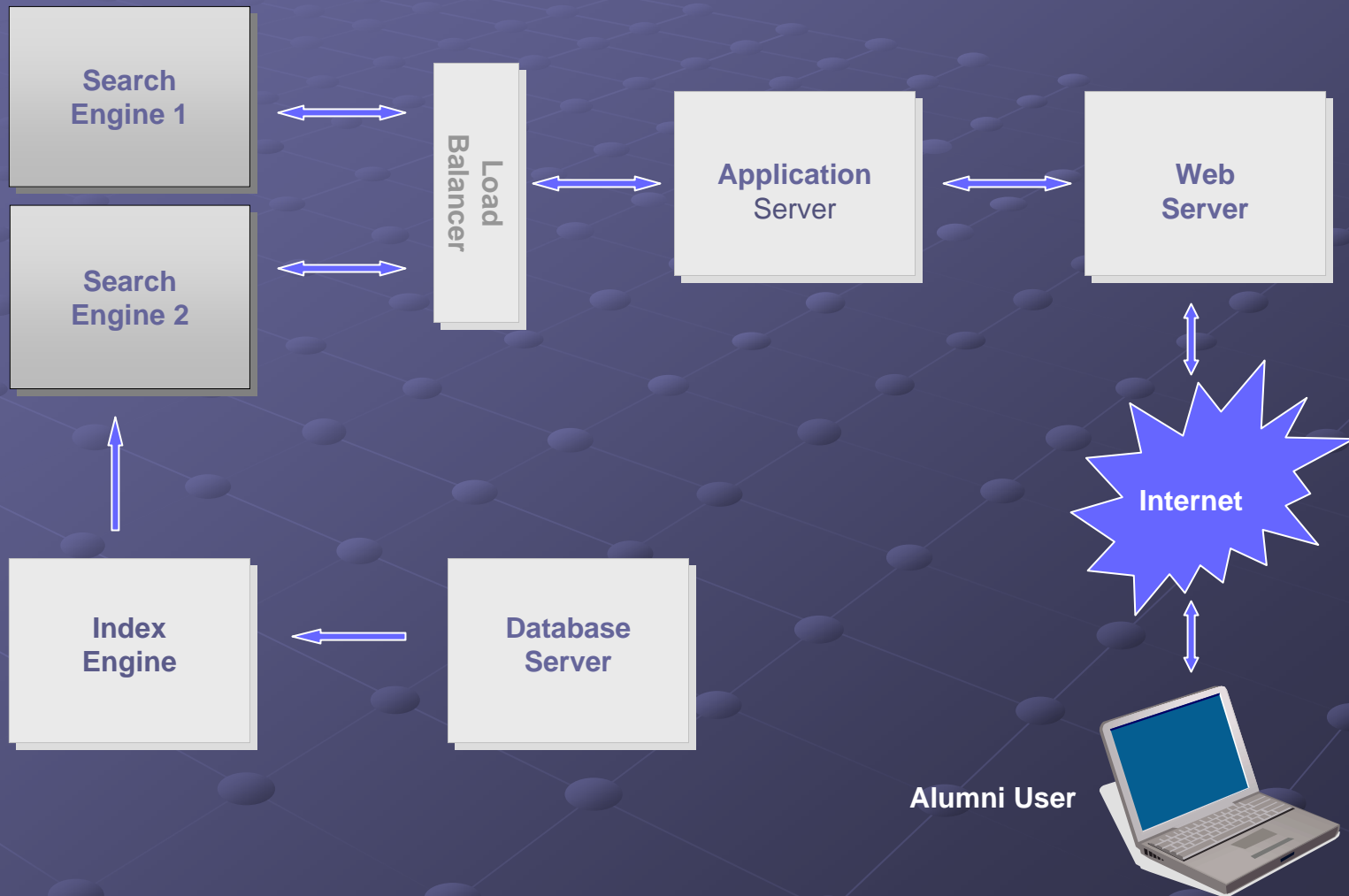
The left sidebar contains a search box with "SEARCH" and "SEARCH WITHIN RESULTS" buttons, and a "Refine Search by Category" section with tabs for "MIT", "Work", and "Home". Under "MIT", there are checkboxes for "Course", "Degree", "Living Group", "Student Activity", "Sports", "Club Membership", and "Volunteer Group". Below this are "QUICK LINKS" for "Make a Gift", "Class Notes", "Tech Reunions", and "Events Calendar". At the bottom of the sidebar is the "INFINITE CONNECTION" section with links for "Email Forwarding", "Alumni Directory", "Update Your Info", and "Mailing Lists".

The main content area also includes a "Filters" section with a "Year of Graduation" filter set to "2000 - 2005" and a "Sort By" dropdown set to "Last Name (A-Z), then First Name" with a "SORT" button. A "Go To Page" section shows a range of page numbers from 1 to 20, with "Next Page" and "Previous Page" links.

The search results list four entries:

- Abbott, Erik CE '00** [Update Record] [Add ICAN Advisor]
Advance ID: 2001019320
Department: CE - Civil Engineering
Degrees: 2000, MNG - Master Of Engrng, Course 1P - Civ&Env Eng Mas Eng
Home Address: Newport Beach CA 92663
Company: Citrix Systems
Job Title: Senior Sales Engineer
Work Address: Newport Beach CA 92663
- Abhyankar, Hari GM '00** [Update Record] [Add ICAN Advisor]
Advance ID: 2001020271
Department: GM - Management
Degrees: 2000, PHD - Doctor Of Phil, Course 15D - Management Doctoral
- Aboumrads, Jouman CE '00** [Update Record] [Add ICAN Advisor]
Advance ID: 2001017104
Department: CE - Civil Engineering
Degrees: 2000, SM - Master Of Science, Course 1M - Civ&Env Eng Sm/Eng
Home Address: Beirut, Lebanon
- Abu-Khalil, Ramy '00** [Update Record] [Add ICAN Advisor]
Advance ID: 1996211523
Degrees: 2000, SB - Bachelor Of Science, Course 2 - Mechanical Engrg

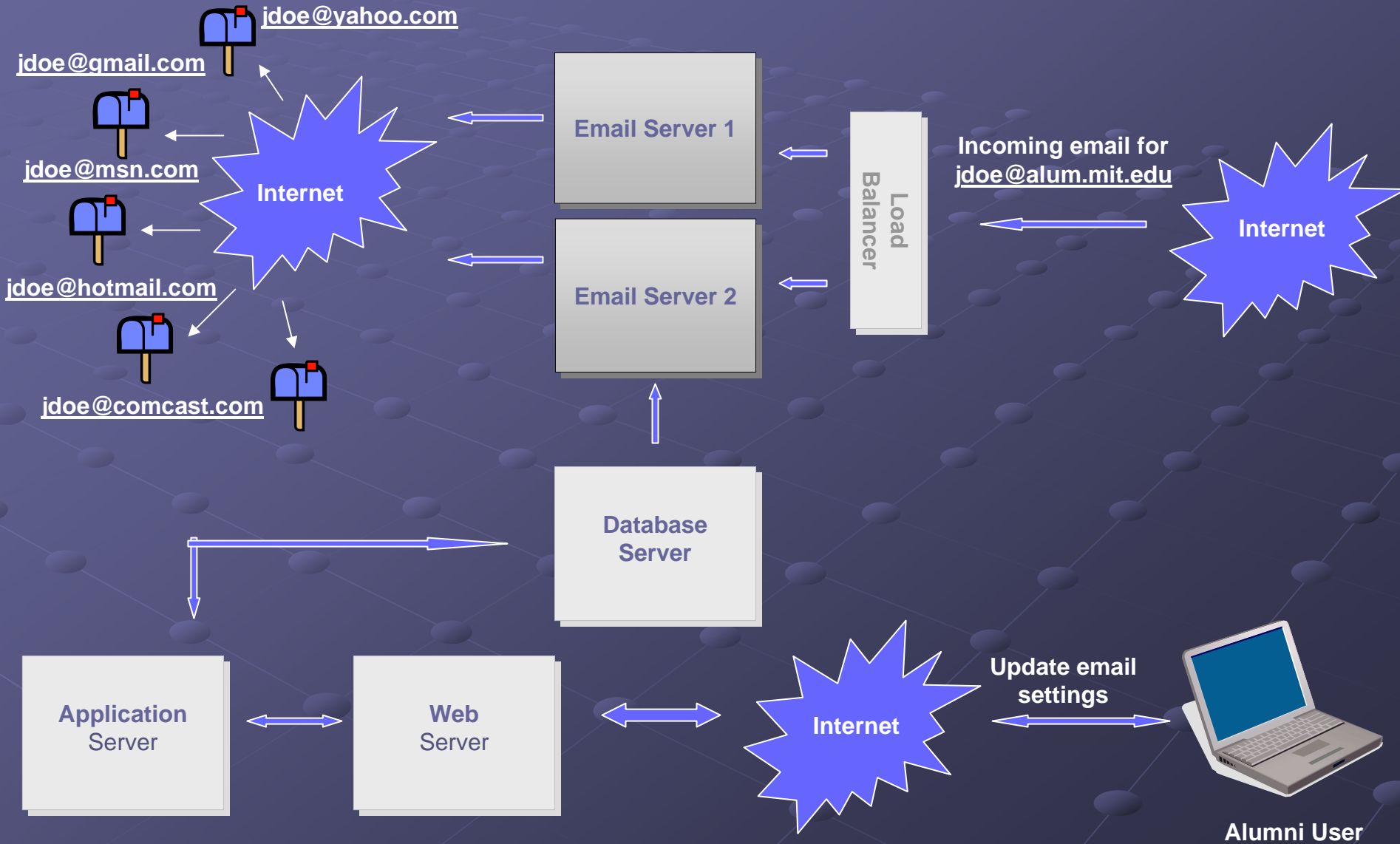
Online Alumni Directory



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

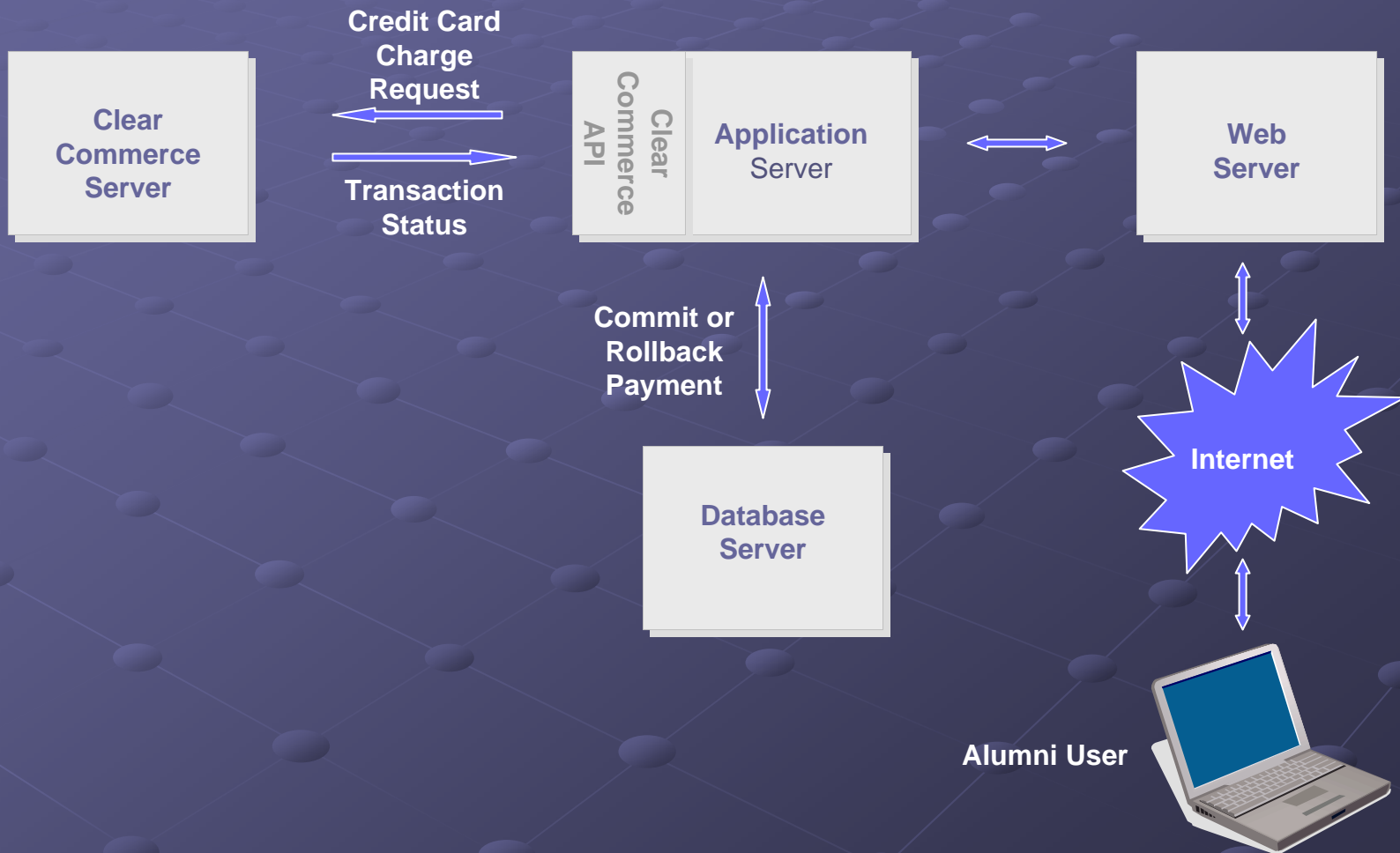
Email Forwarding for Life



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

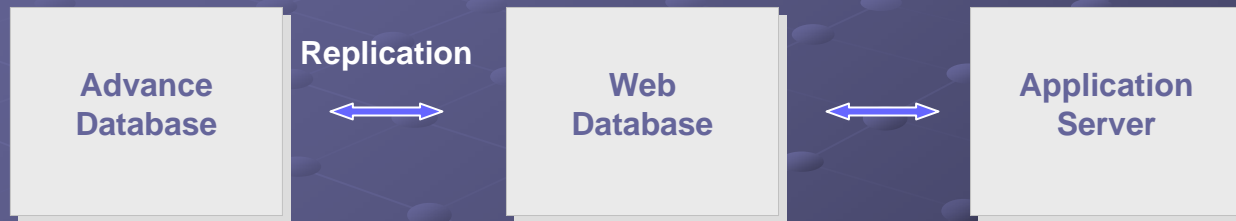


Security Matters

- 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 UTexas (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

