eChat

Bringing Secure Communication to the Next Level

Product for the Present and Future

- Encrypted instant messaging program
- For small- to medium-sized businesses
  - Ensures secure communication over wired AND wireless networks
  - At a low cost

What Makes Us Stand Out

- A relatively light-weight client
- A better, more professional user interface
- Affordability
- No ads

More Benefits

- Features that are relevant to businesses
  - Secure RSA encrypted messages and files communication
  - Grouped and location-independent contact lists
  - User profiles with business contact information
  - Group conference messaging
 - Server-side logging and archiving

How will it work?

- An extension of the open source *ZX2C4 Instant Messenger* program
- A Client-Server architecture
- Encryption algorithms
  - RSA public key/private key
  - AES symmetric key
  - MD5 one-way hash

Client

- Sign-In Window
- Contact List Window
- Instant Messaging Window
- File Transfer Window
- Profile Window
- Preferences Window
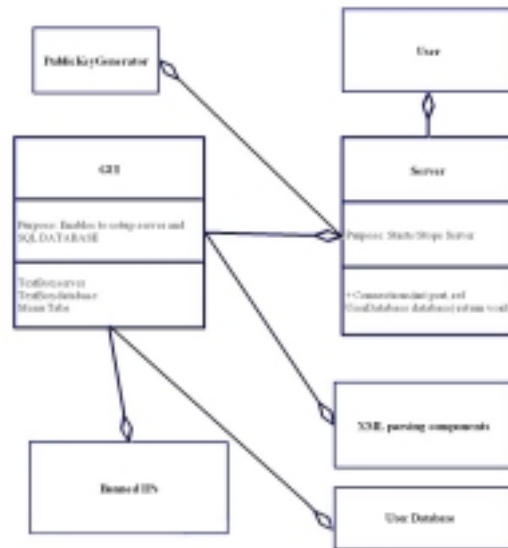- Logs Window

CLIENT DIAGRAM
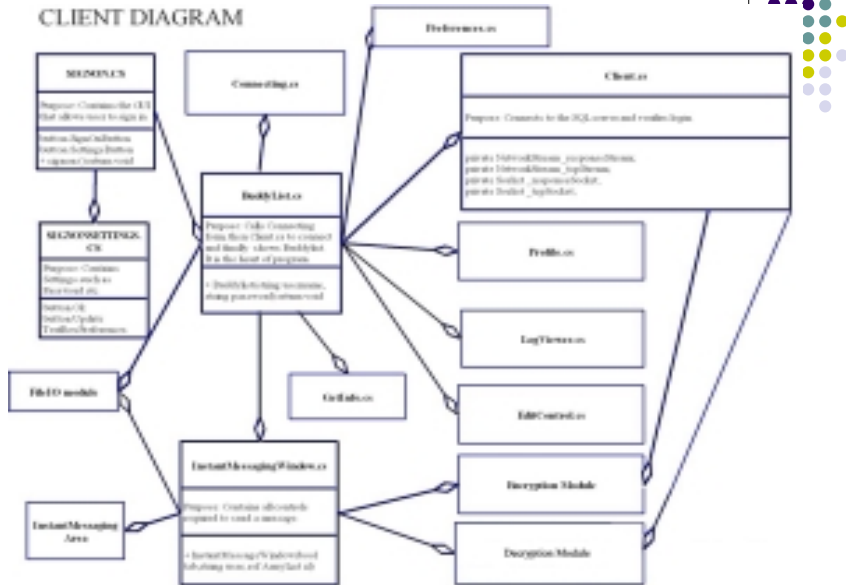
Server

- GUI Module
  - Sign-In Window
  - Main Admin Window: Port#, Start, Stop
  - SQL Settings Dialogue Box
- Database Module
  - Username
  - Password
  - Profile
  - Status
  - Away Message
  - Contact List
  - AES Session Key

Slide 1 — Server Diagram

SERVER DIAGRAM

Slide 2 — Cryptography

Cryptography

- Encryption/Decryption/One Way Hash Module
  - RSA
    - 1024-bit public/private keys for server
  - AES
    - 128-bit symmetric keys shared by client and server
  - MD5
    - 128-bit hashes to check message integrity and generate symmetric keys

Slide 3 — System Requirements

System Requirements

Minimum Client Requirements
- Microsoft Windows 2000 operating system or better
- 300 MHz processor
- 128 MB RAM
- ~2 MB hard disk space for the client, and ~24 MB for the (optional) .NET Framework Redistributable Package v1.1
- Internet connection (56Kbps or faster)

Minimum Server Requirements
- Microsoft Windows 2000 operating system or better
- Microsoft SQL Server 2000
- 500 MHz processor
- 256 MB RAM
- 5 GB hard disk space
- Internet connection (300Mbps or faster)

Slide 4 — WILL it work?

WILL it work?

- Areas of largest risk
  - Speed
  - Existing ZIM bugs
  - No comments in existing code
- A well-planned schedule

Schedule

- http://tinyurl.com/6vfv2

Any Questions?