iLabs Service Broker Complete Machine Build

Author: Chris Felknor and Kirky DeLong

Last Modified: 2/21/07

By: Chris Felknor

Table of Contents

Overview

This document describes the steps necessary to build an iLabs development machine from **scratch** on the Windows platform. It covers the installation of Windows Server 2003, SQL Server, Visual Studio.NET 2003, and various tools. It also describes the installation of the iLabs source code and the creation of a development project in Visual Studio.NET

Requirements

You should have the following materials on hand before you begin:

- Windows 2003 Server Enterprise Edition CD
  - SATA Drivers on a floppy disk (if your system has a SATA drive)
  - SCSI and/or RAID Drivers on a floppy disk (if applicable to your system)
- SQL Server 2000 CD
- SQL Server 2000 Service Pack 3a CD
- Visual Studio.NET 2003 Professional and Library (6 CDs)
- ILabs Service Broker Code zip files (the latest version can be downloaded from http://icampus.mit.edu/iLabs/architecture)

Windows Server 2003

Base Installation

To get a clean install, the partition the operating system resides on will be reformatted. The only way to accomplish this is to boot from an installation CD.

Insert the Windows 2003 CD and restart the computer. Watch for a message at the top of the screen that says “Press any key to boot from CD..”. If you miss this message, you will have to turn off the machine and try again. If you do not see this message at all, you will have to go into CMOS setup and enable the CD-ROM drive as a boot device.

Note: **Do not connect the computer to the network until the very end of the build process**. This is to prevent the machine from being hacked until it is properly secured and also to make it easier to reboot with a (temporarily) blank Administrator password.

Once the machine begins to boot, it can take 2 or 3 minutes to load all of the drivers for Windows.

SATA, SCSI, or RAID Drives

If you have a SCSI or SATA drive, or a RAID controller, watch for the prompt that says **Press F6 if you need to load a SCSI or RAID Driver**. When it has finished initializing, follow the instructions below.

√	Screen Text	Notes	Your Response
	Windows Setup Setup could not determine the type of one or more mass storage devices installed in your system, or you have chosen to manually specify an adapter…"	Pertains to **SCSI, SATA, or RAID** devices only. If you do not have one of these devices, skip to the **Welcome to Setup** step.	Press **S** to Specify an Additional Devide
	Windows Setup Please insert the disk labeled Manufacturer-supplied hardware support disk into Drive A:		Insert your driver diskette into Drive A. (It does not have to be labeled "Manufacturer-supplied hardware support"). Press **Enter** when ready.
	Windows Setup You have chosen to configure a SCSI Adapter for use with Windows, using a device support disk provided by an adapter manufacturer.	You should be presented with a menu of the device drivers that are available on the diskette.	Select the correct driver on the menu and press **Enter**. You should see a message that says that the drivers are being loaded.
	Windows Setup Setup will load support for the following mass storage device(s):…		Press **Enter** to continue. If you have additional drivers to load, you can press **S** here and go through the procedure again.
	Welcome to Setup This portion of the Setup program prepares Microsoft ® Windows ® to run on your computer. • To set up Windows now, press Enter • To repair a Windows installation using Recovery Console, press R. • To quit Setup without installing Windows, press F3		**Enter**
	Windows Licensing Agreement		**Hit F8** to agree to the licensing agreement and continue.
	If one of the following Windows installations is damaged, Setup can try to repair it. Use the UP and DOWN ARROW keys to select an installation. • To repair the selected Windows installation, press R • To continue installing a fresh copy of Windows without repairing, press ESC	**This screen only comes up if you are replacing a previous installation**. In order to make sure you are starting with a clean build, you should always choose to install a fresh copy without repairing	**Press ESC**
	FDISK Screen The following list shows the existing partitions and unpartitioned space on this computer. Use the UP and DOWN ARROW keys to select an item in the list. • To set up Windows on the select item, press Enter. • To create a partition in the unpartitioned space, press C	On the next few screens, we will delete all of the partitions on the machine, and recreate them as follows: • C – 20 gig (Operating System) • D – remaining space (Data)	Select the C partition and **press D** to delete it. See the next screen to continue…

	• To delete the highlighted partition, press D		
	The partition you tried to delete is a system partition... • To delete this partition, press ENTER. • To go back to the previous screen without deleting the partition, press ESC		**Press Enter** Another screen appears cautioning you that all data on the C partition will be lost if you continue. **Press L**
	The following list shows the existing partitions and unpartitioned space on this computer. Use the UP and DOWN ARROW keys to select an item in the list. • To set up Windows on the select item, press Enter. • To create a partition in the unpartitioned space, press C • To delete the highlighted partition, press D	If there are any more partitions on the drive, delete them now (unless you have a pre-existing data drive that you want to keep).	Select the D (or E, etc.) partition and **press D** to delete it. Another screen appears cautioning you that all data on the D (or E, etc.) partition will be lost if you continue. **Press L**
	The following list shows the existing partitions and unpartitioned space on this computer. Use the UP and DOWN ARROW keys to select an item in the list. • To set up Windows on the select item, press Enter. • To create a partition in the unpartitioned space, press C • To delete the highlighted partition, press D	At this point you should have nothing but unpartitioned space, unless you have opted to preserve data on a one of the non-operating system partitions. Now you must recreate the C Partition.	**Select** the line that says "**Unpartitioned Space**", where the C Drive used to be. **Press C**
	You have asked Setup to create a new partition on [disk info] • To create the new partition, enter a size below and press ENTER • To return to the previous screen without creating the partition, press ESC The minimum size for the new partition is (n) (MB) The maximum size for the new partition is (n) (MB) Create a partition of size (in MB): n		Key in 20000 Megabytes for a 20-gigabyte partition. **Press Enter** **NOTE:** If you have a small hard drive (for example, on a laptop), you can change the partition size to 10 gigabytes (10000 Megabytes). Or, you may choose to only have one partition, the C Drive. In that case, do not create another partition for D, and substitute "C" for "D" in subsequent parts of this document where specific path names are mentioned.
	The following list shows the existing partitions and unpartitioned space on this computer. Use the UP and DOWN ARROW keys to select an item in the list. • To set up Windows on the select item, press Enter. • To create a partition in the unpartitioned space, press C • To delete the highlighted	Create a partition (D) for data, using the rest of the Unpartitioned Space.	**Select** the line that says "**Unpartitioned Space**" **Press C**

	partition, press D		
	You have asked Setup to create a new partition on [disk info] • To create the new partition, enter a size below and press ENTER • To return to the previous screen without creating the partition, press ESC The minimum size for the new partition is (n) (MB) The maximum size for the new partition is (n) (MB) Create a partition of size (in MB): n		Leave the default number in the box, representing the remaining unpartitioned space on the drive. **Press Enter**
	The following list shows the existing partitions and unpartitioned space on this computer. Use the UP and DOWN ARROW keys to select an item in the list. • To set up Windows on the select item, press Enter. • To create a partition in the unpartitioned space, press C To delete the highlighted partition, press D	Now we will set up Windows. The first step is to format the C Partition.	**Select the C partition** (it should say “New (Raw)”). **Press Enter**
	The partition you selected is not formatted. Setup will now format the partition. Use the UP and DOWN ARROW keys to select the file system you want, and then press ENTER. If you want to select a different partition for Windows, press ESC.	**Choosing NTFS is very important** here, as Windows Server cannot set up its full file system security model on the FAT system. Eventually you will not be able to set up a debugging environment in Visual Studio.NET, and you will have to reinstall the operating system. (A FAT partition can be promoted to NTFS, but Windows will not have set the permissions that it does during an installation. Getting that right is more difficult than a base install).	Choose "**Format the partition using the NTFS file system**". Do not choose the Quick Format option. **Press Enter**
	Please wait while Setup formats the partition	There will be a progress bar below with a message that says, "Setup is formatting". This will take a few minutes	Get up and stretch your legs. At this point, the installation will continue unattended until the Regional Settings screen below.
	Please wait while Setup examines your disk. This may take several minutes.		This screen will go by fairly quickly.
	Please wait while Setup copies files to the Windows installation folders. This may take several minutes to complete. [Progress bar that says, "Setup is copying files...]	This concludes the character-based portion of the installation routine. When it completes, the computer will reboot. It will then start Windows and complete setup using a GUI interface. If you have loaded drivers from a floppy diskette, you must remove it before it reboots.	This will take a few minutes.
	Installing Windows There will be a grey screen with the following tasks listed on the left: Collecting Information Dynamic Update Preparing Installation Installing Windows Finalizing Installation	If you have loaded SATA, SCSI, or RAID drivers, you might be prompted to insert your driver disk again.	This will take a few minutes. A message at the bottom of the screen will provide an estimate of the remaining time. After a while, you will see a heading that says “Installing Devices, under which a progress bar appears.
	Regional Settings You can customize Windows for different regions and languages.	This is where you can customize the keyboard layout and system locale.	**Accept defaults.** **Next ->**

	Personalize Your Software Type the full name of your company or organization. **Name: [Machine Name]** **Organization: [MIT]**		Type in the name and Organization. Use the machine name [**MachineName**] for "name". **Next ->**
	Your product key		Enter the MSDN Product Key: **Next ->**
	Licensing Modes		Choose **Per Device or Per User** **Next->**
	Computer Name and Administrator Password **Computer Name: [**MachineName**]** **[Leave the Administrator password blank for now.]**		**[Next ->]**
	You have not specified a password for the Administrator Account. Are you sure you want to continue without setting a password? Type a password for the Administrator Account. Are you sure you want to continue without setting a password?	You will see this if you leave the Administrator password blank.	Click **Yes**
	Date and Time Settings		**Set the correct date, time and Time Zone.** **Next->**
	Installing Network Please wait while Windows installs networking components.		This will take a few minutes. There is a progress bar as files are copied.
	Networking Settings		Choose **Custom Settings** **Next ->**
	Networking Components	You can set configure your IP address and specify DNS servers here, or you can do it later. The procedure is described under the NIC topic on page 10.	**Next ->**
	Workgroup or Computer Domain		**Choose** No, this computer is not on a network, or is on a network without a domain. Type a workgroup name in the following box. **Workgroup or computer domain:** **WORKGROUP** **Next ->**
	Installing Windows The grey setup screen returns. Progress bar messages: Copying Files... Completing Installation… Installing Start Menu Items... Registering Components... Saving Settings...		This continues without intervention. When it is finished, the machine will reboot. Remove any CD or floppy left in the computer prior to the reboot.
	Logon Screen		Press **Ctrl-Alt-Delete** to logon

	Windows Server Post-Setup Security Updates	This asks you to patch the server and configure automatic updates.	Click **Finish** We will do this later when the computer is connected to the network.
	Manage Your Server	The first time you log on as Administrator, you will see this screen.	**Uncheck** Show this screen at startup. **Close** the window.

Video Driver

If Windows does not include a driver for your video adapter, now is the time to add one. If you do not have a driver CD that came with your computer, you will need to determine the make and model of your video adapter, and download the appropriate driver from the Vendor's web site. Since this machine should not yet be connected to the Internet, this must be done from another machine.

Reboot after the driver has been installed. When the system comes back up, the system will recognize the existence of new hardware if it is a plug-n-play device. You will get the following series of prompts:

Found New Hardware Wizard
This wizard helps you install software for:
(the driver it found)

What do you want the wizard to do?
Choose **Install the software automatically**
Next->

Security alert - Driver Installation
The installed INF file does not contain digital signature information.
Do you still want to install this driver software?
Yes

Completing the Found New Hardware Wizard
Finish

You may have to repeat this process, if more than one driver has been installed. When all of the drivers have been installed, reboot the machine.

After the reboot, your screen settings may have been updated automatically by Windows. If not, do the following:

- Right-click anywhere on the desktop, and select Properties from the pop-up menu
- Click the **Settings** tab in the Display Properties box. From the **Colors** dropdown box below, change the resolution to True Color (32 bit). Under

Screen Area, you can change the sizing of your screen to suit your preference.

- ❑ Click **OK** when finished. A second box will pop up; click **OK**. A third box will appear; click **Yes**

NIC

Hardware

In most cases, Windows will simply recognize your network adapter when it installs. If it does not, however, you will need to add a driver for it. If you do not have a driver CD that came with your computer, you will need to determine the make and model of your NIC, and download the appropriate driver from the Vendor’s web site.

Once you have the correct driver, follow this procedure.

- ❑ Right-click My Computer
- ❑ Properties
- ❑ Hardware Tab
- ❑ **Device Manager** Button
- ❑ Other Devices: Right-Click on **Ethernet Controller**. Should have a yellow question mark in front of it.
- ❑ **Properties**
- ❑ **Reinstall Driver** Button
- ❑ Install from a list or specific location (Advanced)
- ❑ **Next**
- ❑ Don’t search. I will choose the driver to install
- ❑ **Browse** to the location of the driver
- ❑ Click **Open**
- ❑ Click **OK**
- ❑ **Wait** for the following messages:
  The wizard found a driver for the following device: Ethernet Controller. Windows found a driver that is a closer match for this device than your current driver. To install the driver Windows found, click Next.
- ❑ **Next**
- ❑ **Wait** until you get this message: Completing the Upgrade Device Driver Wizard.
- ❑ Click **Finish**
- ❑ Click **Close**
- ❑ Close the Device Manager Window
- ❑ Close the System Properties Window

Configuring Network Software

This is where you will configure the NIC.

Start -> Control Panel -> Network Connections ->Local Area Connection (right-click and select Properties)

- ❑ Scroll down if necessary to the bottom of the list
- ❑ Click on **Internet Protocol (TCP/IP)**
- ❑ Click the **Properties** button
  If you are using DHCP to obtain an IP address, leave “Obtain an IP address automatically” selected. If not, select “Use the following IP address”, and key in your IP address, Subnet mask, and Default gateway.
- ❑ Click the **Advanced** Button at the bottom
- ❑ Click the **DNS** tab
- ❑ Click the **Add**.. button
- ❑ Add your local DNS Servers. Click **Add** after keying in each one, and then re-click the **Add**.. button to add the next one.
- ❑ Now click the WINS tab
- ❑ For security reasons, select **Disable NetBIOS over TCP/IP**
- ❑ Click **OK** when finished.
- ❑ Click **OK** to close the Internet Protocol (TCP/IP) Properties window.
- ❑ Scroll up in the window until you see **File and Printer Sharing for Microsoft Networks**. **Uncheck** the box next to it. **This is an essential security measure for any Windows machine with an Internet facing NIC**. Otherwise, your machine will appear in Network Neighborhood to the world!
- ❑ Click **Close** to close the Local Area Connection Properties window.
- ❑ Click **Yes** if it asks you if you want to restart your computer (Reboot).

Audio Driver

If Windows does not recognize your audio driver, obtain the correct driver and install it now. Reboot when finished.

After the reboot, go to Start-Control Panel->Sounds and Audio Devices. You should see the following message:

“This computer cannot play audio because the Windows Audio service is not enabled”.

- ❑ Check the box next to **Enable Windows Audio** and press OK.
- ❑ Another dialog box will pop up that says “Windows Audio is now enabled, but the changes will not take effect until you restart Windows.” Click **Yes** to reboot.

Internet Information Server (IIS)

In Windows Server 2003, IIS is not installed by default. Since this includes the Web Server, and the means by which ASP.NET pages are served, it must be installed.

Installing the Web Server

- ❑ From the Start menu, click **Mange your Server**
- ❑ Under Adding Roles to Your Server, click **Add or remove a role**
- ❑ On the Preliminary Steps dialog, click **Next >**
- ❑ A message appears: “At least one of the network connections on this server is currently disconnected…” Click **Continue**
- ❑ Configuration Options: Select **Custom Config**, then click **Next>**
- ❑ Under Server Role, click **Application server (IIS, ASP.NET)** and then click **Next>**.
- ❑ Click the boxes next to **Front Page Extensions** and **Enable ASP.NET and then** click **Next >**
- ❑ Review the Summary box, then click **Next >**
- ❑ Insert the Windows Server 2003 CD when prompted
- ❑ Wait while components are installed
- ❑ When it is finished, you will see a message that says **This Server is Now an Application server**
- ❑ Click **Finish**
- ❑ Close the Manage Your Server window

Changing the Default Web Server File Location

Next, change the default file location of the web site and the log files to the D Drive. If you do not have a D drive, skip to the next section, SMTP Server.

- ❑ Format the D Drive:
    - ○ Start->My Computer (Right-click, choose Explore)
    - ○ Right-click on the **D Drive**, select **Format…**
    - ○ Make sure **NTFS** is selected
    - ○ For the **Volume Label**, type **Data**
    - ○ Do not check Quick Format or Enable Compression
    - ○ Click **Start**
    - ○ Click **OK** when the warning window pops up – Formatting will erase all data on this disk.
    - ○ If you have a large partition, this can take some time to complete.
- ❑ Open the Windows Explorer
- ❑ Create a folder called **Inetpub** on the **D Drive**
- ❑ Create a sub-folder of Inetpub called **wwwroot**
- ❑ Create a folder called **Logs** on the **D Drive**
- ❑ Right-Click on Start -> **My Computer**

- □ Select **Manage**
- □ Expand **Services and Applications**
- □ Expand **Internet Information Services**
- □ Expand **Web Sites**
- □ Right-Click **Default Web Site**
- □ Select **Properties**
- □ Click on the **Web Site** tab
- □ Next to **Active log format**, at the bottom, click **Properties**
- □ In the **Log file** Directory box at the bottom, type **D:\Logs**
- □ Click **OK**
- □ Click the **Home Directory** tab at the top
- □ In the **Local Path** box, change the drive letter from **C** to **D** (D:\inetpub\wwwroot)
- □ Click **OK**
- □ Stop and restart IIS by selecting Start->Run and typing **iisreset** on the command line.

SMTP Server

The iLabs Service Broker sends mail for things like help requests and bug reports. For this, you must add the SMTP Server Role to your Windows 2003 server.

Adding the Server Role

- □ Open the Manage Server window. Start -> Manage Your Server
- □ Under Adding Roles to Your Server, click **Add or remove a role**
- □ On the Preliminary Steps dialog, click **Next >**
- □ A message appears: “At least one of the network connections on this server is currently disconnected…” Click **Continue**
- □ Configuration Options: Select **Custom Config**, then click **Next>**
- □ Under Server Role, click **Mail server (POP3, SMTP)**. It should say “no” under “configured”. Click **Next>**.
- □ Authentication Method: select **Local Windows Accounts**
- □ Type in the domain for receiving mail in the mail boxes (this is for POP3; not needed for the iLabs Service Broker. If you have a fully qualified domain name (e.g. machine.domain.edu) type it here; otherwise just enter the machine name).
- □ Click **Next >**
- □ Review the Summary box. It should say “Install POP3 and Simple Mail Transfer Protocol (SMTP) to enable POP3 mail clients to send and receive mail”. Click **Next >**
- □ Insert the Windows Server 2003 CD when prompted. If autoplay brings up a screen that says "Welcome to Microsoft(R) Windows(R) Server 2003", close it.
- □ Wait while components are installed

- □ When it is finished, you will see a message that says **This Server is Now a Mail server**
- □ Click **Finish**
- □ Close the Manage Your Server window

Setting Access Permissions

- □ Start-> Right-Click on **My Computer**
- □ Select **Manage**
- □ Expand **Services and Applications**
- □ Expand **Internet Information Services**
- □ Expand **Default SMTP Virtual Server**
- □ Right-Click **Default SMTP Virtual Server**
- □ Select **Properties**
- □ **Access** tab
- □ **Connection** button
- □ Select which computers may access this virtual server: Make sure the "Only the List Below" option is selected. Click the **Add…** button
- □ Make sure "Single Computer" is selected, and key in IP address **127.0.0.1** to permit only the local machine to access the SMTP server.
- □ Click **OK**
- □ Click **OK** again
- □ Click the **Relay** button
- □ Make sure the "Only the List Below" option is selected. Click the **Add…** button
- □ Make sure "Single Computer" is selected, and key in IP address **127.0.0.1** to permit only the local machine to relay messages through the SMTP server.
- □ Uncheck the box that says "Allow all computers which successfully authenticate to relay, regardless of the list above".
- □ Click **OK**
- □ Click **OK** again
- □ Click **OK** to close the Default SMTP Virtual Server Properties page.

After you install the Service Broker Code, you will need to make sure that the web.config file is updated with the correct email addresses for both the supportMailAddress key and the registrationMailAddress key. If these keys are not entered, you will receive the following error message:

```
Exception: Could not access 'CDO.Message' object.
Inner Exceptions:
Exception has been thrown by the target of an invocation.
At least one of the From or Sender fields is required, and neither was found.
```

Security

Local Security Policy

Open Start->Programs->Administrative Tools->Local Security Policy

These changes will cause various events to be written to the Security Event Log.

Under **Account Policies -> Account Lockout Policy**:

- ❑ Account lockout threshold -> 10 invalid login attempts
- ❑ Account lockout duration -> 30 minutes
- ❑ Reset account lockout after -> 30 minutes

Under **Local Policies -> Audit Policy**

- ❑ Audit account logon events -> Success, Failure
- ❑ Audit account management -> Failure
- ❑ Audit directory service access -> Failure
- ❑ Audit logon events -> Failure
- ❑ Audit object access - > No auditing
- ❑ Audit policy change -> Success, Failure
- ❑ Audit privilege use -> No auditing
- ❑ Audit process tracking -> No auditing
- ❑ Audit system events -> Failure

Close the Local Security Settings Window

Windows Firewall

Windows Server 2003 ships with a firewall feature. This should be enabled for security.

Start -> Control Panel -> Network Connections -> Local Area Connection (right-click, select Properties)

- ❑ On the Local Area Connection Properties sheet, click the **Advanced** tab.
- ❑ Check the box next to **Protect my computer and network…**
- ❑ Click the **Settings** button
- ❑ Select the **General** tab and turn the firewall **ON**
- ❑ Select the **Exceptions** tab and click the box next to **Remote Desktop** (if you intend to use Terminal Services to access the machine remotely)
- ❑ Select the **Advanced** tab
- ❑ In the **Network Connection Settings** area make sure the Local Area Connection box is checked and click on **Settings**
- ❑ In the **Services** tab, click the box next to **Web Server (HTTP)**

- ❑ Select the default for the Name or IP address of the computer hosting this service on your network; click **OK**.
- ❑ Click the box next to **Remote Desktop** and select the default for the Name or IP address; click **OK**
- ❑ Click the box next to **Secure Web Server (HTTPS)** and select the default for the Name or IP address of the computer hosting this service on your network; click **OK**.
- ❑ Leave the other boxes unchecked (or check the service you want to use, such as FTP)
- ❑ Click **OK** to close the settings.
- ❑ Click **OK** to close the Advanced Settings Box.
- ❑ Click **OK** to close the Local Area Connection Properties Box.

Settings

Remote Desktop

To log on to this server remotely, you will need to enable Remote Desktop.

- ❑ Right-click **My Computer**, select **Properties**
- ❑ Click the **Remote** tab
- ❑ Check the box next to **Enable Remote Desktop on this computer**
- ❑ Click **OK** when the information box pops up letting you know that some accounts might not have password.
- ❑ Click **OK** to close the Properties window.
- ❑ You won’t need to add specific users unless you want individuals who do not have Administrator privileges to log on remotely.

SQL Server 2000 Enterprise

SQL User Account

Before installing SQL/2000, create a user account for SQL/2000 Services.

- ❑ Right-Click on **My Computer**
- ❑ Click **Manage**
- ❑ Expand **Local Users and Groups**
- ❑ Right-Click **Users**
- ❑ Click **New User…**
- ❑ User name & Full name: **SqlAccount**
- ❑ Description: **Account for SQL Services**
- ❑ Password: Type a strong password (at least 10 characters long, includes upper case and lower case characters as well as numbers or special characters). Note: there is a good freeware utility to generate strong

passwords called **rpgen**, available here: http://www.paehl.de/rpgen.zip Make sure you keep track of the passwords.

- ❑ Uncheck **User must change password at next logon**
- ❑ Check **User cannot change password**
- ❑ Check **Password never expires**
- ❑ Click **Create**
- ❑ Click **Close**

Base Product

Before installing SQL Server, create a folder on the D Drive to contain the data.

- ❑ On the D Drive, create a folder called **Database**
- ❑ Open this folder and create a sub-folder called **Data**
- ❑ In the Database folder, create another sub-folder called **Backup**

Place the SQL Server 2000 Enterprise CD in the CD Drive.

- ❑ The installation program should load automatically. If it does not, Navigate to <CD Drive>:\ENGLISH\ENT and Double-click **Autorun.exe**
- ❑ Click **SQL Server 2000 Components**
- ❑ Click **Install Database Server**
- ❑ You will see an error message: **SQL Server 2000 SP2 and below**. We will fix this later; for now, click **Continue**
- ❑ Welcome to the Microsoft SQL Server Installation Wizard. **Next->**
- ❑ Accept the default of **Local Computer**. **Next ->**
- ❑ Accept the default of **Create a new instance of SQL Server… Next ->**
- ❑ For name, enter the Machine Name. For Company, enter your university or company name. **Next->**
- ❑ Click **Yes** to accept the License agreement
- ❑ Accept the default of **Server and Client Tools**. **Next ->**
- ❑ Leave the box next to **Default** checked. **Next ->**
- ❑ Setup Type: Check the **Custom** radio button
- ❑ Leave the program and Data files in their default location (We will change the data file location later) **Next->**
- ❑ Select Components: Leave the defaults, unless you also want the code samples. Click **Next ->**
- ❑ Service Accounts: **Use the same account** for Each Service. **Use A Domain User Account** – For security reasons, it is a good idea not to run the SQL Server as administrator. Use the SQLAccount user you created earlier for running the SQL Server services. Enter SqlAccount for the username and the password in the correct boxes.
- ❑ **Next ->**
- ❑ Authentication Mode: **Windows Authentication Mode. Next->**
- ❑ Collation Settings: Accept defaults. **Next->**
- ❑ Network Libraries: Accept defaults. **Next->**

- Start Copying Files. Setup has enough information… **Next->**
- Choose Licensing Mode: **Per Seat** for **25** devices. Click **Continue**
- Wait for a while the product is installed.
- **Setup Complete**. When you see this message, click **Finish**.
- Remove the CD, and **Reboot** the machine.

Changing the default file locations

- Click Start-> Enterprise Manager
- Navigate to Console Root->Microsoft SQL Servers->SQL Server Group->Machine Name (may say (local) (Windows NT))
- Right-click on the Server name (or “local”) and click **Properties.**
- Click the **Database Settings** tab.
- Near the bottom, click the … button to the right of the **Default data directory** box. Navigate to D:\Database\Data
- Click **OK**
- Repeat this procedure for the **Default log directory** (note: the log files can go in the same directory as the data files).
- Click OK
- Exit Enterprise Manager

Service Pack 3a

- Insert the SQL Server 2000 Service Pack 3a CD.
- Run **setup.bat** from the root of the CD.
- When the wizard starts, click **Next->**
- Click **Yes** to accept the License Agreement
- Click **Next** to accept the default instance name.
- Click **Next** to accept the default of “The Windows account information I use to log on…”
- Wait while the username is validated.
- Enter SA Password: type a strong password (at least 10 characters long, includes upper case and lower case characters as well as numbers or special characters). Make sure you keep track of the passwords.
- Check the box next to Upgrade Microsoft Search and apply SQL Server 2000 SP3 (required), and click **Continue**
- Error reporting: leave the box unchecked, click **OK**
- Wait until the “Setup is gathering information” message completes
- Start Copying Files. Setup has enough information….**Next ->**
- Wait for a while as Service Pack 3a is installed. This will take a while.
- Ignore the message that says you should backup your master and msdb database. Click **OK**
- Click **Finish**
- Remove the CD, and **Reboot** the machine.

Security Configuration

SQL Server can be an avenue for hackers to gain access to your system, if it is not properly administered. SQL Server security is a big topic, so a comprehensive discussion of it is beyond the scope of this document. We will, however, cover the basics.

Potential Security Breaches

Practically speaking, there are two main ways a hacker can gain access to your system through SQL Server:

Direct Attack

An attacker may try to break into your system directly, by connecting to SQL Server's default TCP port of 1433. If this happens, and you are using SQL or Mixed Authentication, a hacker can use a password grinder to discover your "sa" password (The SQL Authentication built-in administrator account). Once someone has gained access to this account, they can execute operating system commands on your server using the **`xp_cmdshell`** stored procedure built into SQL Server. This is arguably the worst system compromise there is, as someone can then set up shop on your system and do anything you could do as the administrator.

Since we are using Windows Firewall, port 1433 is closed by default. You may want to open this port and connect to your SQL Server from another machine using Enterprise Manager, but this is not advisable unless your machine is on a subnet which is behind a firewall. You should not open port 1433 and allow outside connections to SQL Server on a machine which is exposed to the Internet.

SQL Injection

SQL Injection is used to attack a SQL Server through a web application. It is a process based on making educated guesses about how a web developer constructed the SQL statements which return data to a web page.

A common design pattern is for a developer to accept user input from a web form (for example, customer name), and then use string concatenation to build a SQL statement from that input (e.g. "SELECT * FROM customers WHERE customer_name = " + Request["customerName"]). Since the entire concatenated statement is going to be interpreted by the SQL query engine, what would happen in this example if someone keyed in another SQL statement in place of the customer name? If a hacker guesses correctly, an incredible amount of data can be returned from SQL server, up to and including a dump of every row of every table to the screen.

Defending Against Common Security Breaches

Direct Attack

If you follow these steps, you should never have to worry about direct access to your SQL Server. Note: If you have followed the instructions in this document, these settings should already be in effect.

- ❑ Make sure that Windows Firewall is in effect and that port 1433 is not open.
- ❑ Set up SQL Server to use Windows Authentication, not Mixed Authentication.
- ❑ Configure SQL Server to run as a non-privileged user (We have already created such a user, SqlAccount). Do not allow SQL Server to run under the SYSTEM account, or an account with Administrator privileges.

SQL Injection

The bad news about SQL injection is that there is no way to configure your server to defend against it; it is completely dependent on the coding practices of your web site's developers. The way to guard against SQL injection attacks is to use parameterized SQL statements in the code, rather than build SQL statements by concatenating them with user input from a web site. If SQL parameters are used, input data is treated as literal data and never as part of a statement. Also, strict type-checking is done.

The good news is that a SQL injection attack cannot do much to damage your system since an ASP.NET web site runs under a less privileged account, which does not have permission to execute **`xp_cmdshell`**. The risk with SQL injection lies in having your data exposed and stolen.

Other SQL Configurations

Following are some other recommended security options for SQL Server.

- ❑ Remove the sample databases (Northwind, Pubs)
  1) Open Enterprise Manager: Start-> Enterprise Manager
  2) Expand the tree at left to show Databases: Console Root -> Microsoft SQL Servers -> SQL Server Group -> (local) (or ServerName) -> Databases
  3) Find **Northwind** in the list of databases.
  4) Right-click on Northwind, and select **Delete**
  5) Click "Yes" on the "Are you Sure" prompt
  6) Delete the **pubs** database, as above.
- ❑ Enable SQL Server login auditing.
  1) Open Enterprise Manager: Start-> Enterprise Manager
  2) Select the root of your SQL Server ("(local)" or the server name).

3) Right-click and select **Properties.**
4) Select the **Security** tab
5) Set Audit Level to **"Failure"**. This will show failed SQL Logins in the Application Event log (if you have port 1433 open to the Internet, you will probably see hundreds of them).

- ❑ To view events in the Application Event Log
  1) Right-Click on **My Computer**
  2) Open **System Tools->Event Viewer-Application**
  3) Look at entries for MSSQLSERVER

Finishing Tasks

User Accounts

Create a new Administrator account as follows:

- ❑ Right-Click on **My Computer**
- ❑ Click **Manage**
- ❑ Expand **Local Users and Groups**
- ❑ Right-Click **Users**
- ❑ Click **New User…**
- ❑ User name & Full name: **YourAccountName**
- ❑ Password: Type a strong password (at least 10 characters long, includes upper case and lower case characters as well as numbers or special characters). Note: there is a good freeware utility to generate strong passwords called **rpgen**, available here: http://www.paehl.de/rpgen.zip
- ❑ Uncheck **User must change password at next logon**
- ❑ Click **Create**
- ❑ Click **Close**
- ❑ In the right panel, Right-click the newly-created user
- ❑ Click **Properties**
- ❑ Click the **Member Of** tab
- ❑ Click **Add**
- ❑ Type **Administrators**
- ❑ Click **Check Names**. Your typing should be replaced with [MachineName]\ADMINISTRATORS
- ❑ Click **Add**
- ❑ Click **OK**
- ❑ Click **OK**

Rename the Administrator Account

Change the built-in Administrator's permissions to "Guest". Use the **Member Of** tab as described above.

Reset the built-in Administrator's password to a strong password: At least 10 characters, using mixed case characters, numbers, and special characters.

Legal Notice

A legal notice at sign-on serves both as a warning to hackers, and as an impediment to password grinders.

To create your own notice, open Regedit to the following path:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`
There are two keys:

`LegalNoticeCaption` (what appears on the top of the window). Good choice for this are “Notice”, “Attention”, “Warning”, etc..

`LegalNoticeText` (the legal notice itself)

Here is an example of a legal notice:

Unauthorized attempts to defeat or circumvent security features, to use this computer for other than its intended purposes, to deny service to authorized users, to access, alter, obtain, damage or destroy information, or otherwise to interfere with this computer or its operation are prohibited. Evidence of such acts may be disclosed to law enforcement authorities and result in criminal prosecution under applicable criminal laws.

Explorer Settings

Under **Tools->Folder Options**, click the **View** Tab. Change the settings to your liking, click **Apply**, then click the **Like Current Folder** button. Click **Yes** on the dialog box that pops up. Click **OK** to close the box.

Optionally, rename My Computer to the machine’s name. This helps you keep track of which machine you are accessing when using remote desktop.

Anti-Virus Software

It is a good idea to install one of the commercial anti-virus software packages. Good choices are McAfee or Norton (Symantic).

Disk Image

Before continuing, if possible, create a disk image of your operating system build, using Norton Ghost or a comparable product. While not strictly necessary, this will save a great deal of time in the event that a rebuild of the operating system becomes necessary. If your system is broken into by hackers, infested with spyware, etc. this is the most reliable method of removing all traces of malicious code that may have been hidden on your hard drive. Doing this before connecting to the network increases the odds that your build is virus-free.

Incidentally, one of the main reasons for keeping all data on a separate partition from the operating system is to make it fairly easy to rebuild the operating system should it become corrupt, overly bloated, etc.

Connect to the Network

You may now connect the NIC to the network.

Windows Update

The first thing you should do after connecting to the Network is to run Windows Update. This will insure that your machine has the latest Windows patches.

- ❑ Start-> Help and Support -> **Windows Update**
- ❑ Do you want to install and run Windows Update… **Yes**
- ❑ **Scan for Updates**
- ❑ **Review and Install Updates**
- ❑ Windows Update will have selected all Critical Updates and Service Packs. If you want to look at the other options under Windows Server 2003 or Driver Updates, you may do so, but this is not strictly necessary. If you do, select the ones you want to install with the **Add** button. When finished, click once again on **Review and Install Updates**
- ❑ Click **Install Now**
- ❑ Wait as the updates are downloaded from the Internet.
- ❑ Most likely, there will be a message asking you to reboot. Click **OK**

Note: You may have to run update two times if any of the patches have to be applied separately.

After you have updated and rebooted your system, set it to check for Windows Updates automatically.

- ❑ Start-> Control Panel -> System -> **Automatic Updates** tab
- ❑ Check the box next to **Keep my computer up to date**
- ❑ Check the radio button next to **Notify me before installing any updates and notify me again before installing them on my computer**
- ❑ Click **OK**

Activate Windows

- ❑ Start-> All Programs -> **Activate Windows**
- ❑ Click the radio button next to "**Yes**, let's activate Windows over the Internet now"
- ❑ Click **Next>**
- ❑ Click the radio button next to "**No**, I don't want to register now"

- Click **Next>**
- You should see a message: “You have successfully activated your copy of Windows”.
- Click OK

ILabs Project

There are two different iLabs code distribution zip files that can be downloaded from http://icampus.mit.edu/iLabs/architecture/:

- For a production instance of the Service Broker which will contain compiled dlls and web pages only, select **serviceBrokerXx.zip**
- If you intend to set up a development environment with full source code, select **serviceBrokerXx.SDK.zip**
- **Where Xx is the latest version number.**

In Addition to the Service Broker zip file, you will need the files used to support the tree control dll used in Grant administration, Microsoft.Web.UI.WebControls.dll. These files are supplied in an archive called **webctrl_client.zip**.

Service Broker Source Code

- Create a folder called **MIT iCampus** on the D Drive
- Create a subfolder within MIT iCampus called **iLabs**
- Unzip the iLabs Distribution archive **serviceBrokerXx.zip** or **serviceBrokerXx.SDK.zip** into this folder.
    - Right-click on the zip file
    - Select **Extract All…**
    - Click **Next>**
    - If you are using serviceBroker**Xx**.zip, Leave the default directory; but if you are using serviceBroker**Xx**.SDK.zip, edit the directory to remove the “.SDK” designation, so that it simply reads “D:\MIT iCampus\iLabs\serviceBroker**Xx**”. Click **Next>**
    - Click **Finish**
- Unzip the distribution file **webctrl_client.zip** into the **D:\Inetpub\wwwroot** directory.
    - Right-click on the zip file
    - Select **Extract All…**
    - Click **Next>**
    - Leave the default directory. Click **Next>**
    - Click **Finish**

    You should now have a directory structure that looks like D:\Inetpub\wwwroot\web_client\1.0\… If you only have a \1.0\… directory, you dragged-n-dropped the folder from the zip and did

not extract it. The Tree Control will not find its images unless this path is correct.

Service Broker Web Site

Virtual Directory

First, create a virtual directory in IIS.

- ❑ Right-Click on **My Computer** (renamed to your computer name)
- ❑ Click **Manage**
- ❑ Expand **Services and Applications**
- ❑ Expand **Internet Information Services**
- ❑ Expand **Web Sites**
- ❑ Expand **Default Web Site**
- ❑ Right-click on **Default Web Site**
- ❑ Select New->Virtual Directory
- ❑ Click **Next** in the Virtual Directory Creation Wizard
- ❑ In the Alias box, type **ServiceBroker**
- ❑ Click **Next**
- ❑ Enter **D:\MIT iCampus\iLabs\serviceBrokerXx\www** in the Directory box (or click the Browse button, and navigate to the location where your Service Broker code is)
- ❑ Click **Next**
- ❑ Access Permissions: make sure you check the Run Scripts, Execute and Read permission boxes
- ❑ Click **Next**
- ❑ Click **Finish**
- ❑ You should see the Service Broker site listed under the Default Web Site
- ❑ Close the Computer Management Window

Database

Follow this procedure to create a fresh instance of the iLabs database on your SQL Server:

Create the Database

- ❑ Start-> **Enterprise Manager**
- ❑ Console Root->Microsoft SQL Servers->SQL Server Group->(local)->**Databases**
- ❑ First, create the database. Right-Click on **Databases**
- ❑ **New Database…**
- ❑ Name: **ilabdb6** (You can use any name you would like but you must update the web.config file to use this name)
- ❑ Click **OK**

Grant Access to the Database

- ❑ Expand the **Security** folder in Enterprise Manager.
- ❑ Right-click **Logins**, select **New Login…**
- ❑ In the Name box, type **NT AUTHORITY\NETWORK SERVICE**
  Note: if you already have a login for NT AUTHORITY\NETWORK SERVICE, right-click on it and continue with the next step.
- ❑ Click the **Database Access** tab
- ❑ Check the box next to **ilabdb6** (or the database name you used above)
- ❑ In the box below, click the box next to **db_owner**
- ❑ Click **OK**

Run the Database Scripts

- ❑ Select the **ilabdb6** database (or what you named it) in Enterprise Manager.
- ❑ On the menu bar, Select Tools -> **SQL Query Analyzer**
- ❑ In Query Analyzer, Click File->Open…
  Browse to database scripts directory typically (**D:\MIT iCampus\iLabs\serviceBrokerXx\DB_Scripts)** and open **1.DropAndCreateILabDBTables.sql**
- ❑ Make sure the correct database **ilabdb6** is the selected database in the dropdown at the top, then click the green triangle "play" button to run the script
- ❑ You should see a message about "The command(s) completed Successfully."
- ❑ Open and run **2.DropAndCreateStoredProcedures.sql**, as above
- ❑ You should again see a message about "The command(s) completed Successfully."
- ❑ Open and run **3.SetTableDefaultValues.sql** as above
- ❑ You should see a lot of messages about "1 row(s) affected." and "Checking Identity Information …."
- ❑ Now we will run the new ticketing scripts. In Query Analyzer, click File->Open, and double click on the Ticketing folder. Then open and run **CreateTablesforTK.sql**.
- ❑ You should see a message about "The command(s) completed Successfully."
- ❑ Open and run **CreateStoredProceduresforTK.sql**, as above.
- ❑ You should again see a message about "The command(s) completed Successfully."
- ❑ Open and run **SetDefaultvaluesforTK.sql**, as above.
- ❑ You should see a lot of messages about "1 row(s) affected." and "Checking Identity Information …."
- ❑ Close SQL Query Manager and Enterprise Manager

Web.Config

Web.config is a text file containing configuration information in XML format, residing in the root of the Service Broker web site (typically in the D:\MIT iCampus\iLabs\serviceBrokerXx\www directory). Web.config.template ships with this release. Copy web.config.template to web.config and edit it using notepad. Following is an overview of some of the values you must edit, but for a complete discussion of the contents of web.config please refer to the **Service Broker Configuration.doc** document located in the /serviceBrokerXx/documents/installDocs directory.

Set the Service Broker’s ID

Every Service Broker must have a unique identifier called a GUID. To set your Service Broker’s GUID update the web.config and set the sbGID.

```
<add key="sbGID" value="" />
```

You MUST set sbGID to a GUID (Globally Unique Identifier) which will identify this particular Service Broker to all lab servers. You will need to supply this GUID to the Lab Server(s) administrator so that the lab Server can be configured to communicate with this Service Broker. We use a GUID produced on the ServiceBroker's machine with all the '-', '{', and '}' characters stripped out. A utility program called CreateGUID.exe has been provided for this purpose, found in the Utilities directory of the distribution package. Generate a GUID using this program, then cut and paste it into the value portion of the sbGID key (between the quote marks). Alternately, obtain a GUID by running **GuidGen.exe**. If you have installed Visual Studio.NET 2003, select Tools->Create GUID (or, outside of Visual Studio, browse to GuidGen’s location: C:\Program Files\Microsoft Visual Studio.NET 2003\Common7\Tools\GuidGen.exe). Select **Registry Format**, Click the **Copy** button, and paste the resulting GUID into the web.config file. Then edit out the brackets and dashes. When you have finished, it should look something like this: `<add key="sbGID" value="96430B0517554de38372244A1EA38C4B" />`.

Update the Database Name

Update the database connection variable in the web.config file to use the name you chose when you created the database.

```
<add key=”sqlConnection”
value="data source=(local);initial catalog=iLabDB6;Integrated Security = SSPI" />
```

Update Email Addresses

Do not forget to update the email address keys or else users will encounter errors when registering and sending bugs.

```
<add key="supportMailAddress" value="" />
```

```
<add key="registrationMailAddress" value="" />
```

There are several other parameters that you should be aware of in web.config, for example the email address that bug reports will be sent to. For more detailed information on the settings that will need to be changed in this file, please see **Service Broker Configuration.doc** document located in the /serviceBrokerXx/documents/installDocs directory. This document also contains information about changing the look of the Service Broker.

Testing Your Installation

- Open Internet Explorer
- Browse to http://localhost/ServiceBroker
- Log in as follows:
  - Username: **superUser**
  - Password: **ilab**

Error Messages

When testing your installation of the Service Broker you may see one of the following error messages:

- “*Cannot open database requested in login 'ilabdb6x'. Login fails. Login failed for user 'NT AUTHORITY\NETWORK SERVICE'.*” Edit the web.config and enter the correct database name.
- “The page cannot be displayed. You have attempted to execute a CGI, ISAPI, or other executable program from a directory that does not allow programs to be executed.” The Virtual Directory in IIS does not have the correct permissions. Remove the virtual directory and recreate it with the correct permissions, as explained in the Virtual Directory section on p. 22 (see Access Permissions) Alternately, you can just open the property sheet for the Virtual Directory and check the correct boxes.
- In the System News and Messages section of the login page you may see one of the following messages:
  - An Administrator needs to edit web.config and add a valid Service Broker identifying GUID to the sbGID key in appSettings. Failure to do this may cause web service calls to lab servers that require authentication to fail. In Visual Studio, select Tools->Create Guid. Choose Registry Format, and copy the Guid to the clipboard. Paste the Guid into the sbGID value in web.config, and remove the braces{}.
  - An Administrator needs to edit web.config and add a value for registrationMailAddress. This is the default email address where requests for membership in a group are sent.
  - An Administrator needs to add a value for supportMailAddress. This is the email address where help requests are sent.

To remove error or warning messages from the System News and Message area,

- ❑ Login as superuser
- ❑ Select the Messages tab from the top menu
- ❑ Click on the system bullet in the message type area
- ❑ Select a message to delete and click remove.

Sample Lab

For information on how to configure a Service Broker to work with a sample lab, please see ***Time of Day Sample Lab Server*.doc** located on the iCampus website http://icampus.mit.edu/iLabs/architecture/.

SSL

SSL is optional. The Service Broker does not require the use of SSL. Also, you cannot develop the Service Broker in Visual Studio if it is configured to use SSL.

If you are not planning to use SSL right now, skip to the Visual Studio .NET installation area.

Secure Sockets Layer is a protocol for securing web communications using public/private key cryptography. It uses a private key installed on the server, and a public key installed in the web browser. The keys are installed in certificates.

A server certificate accomplishes (potentially) four tasks:

1) Verifies that the web site the certificate was issued to is the web site that is hosting it (e.g. a certificate issued to "www.mit.edu" is running on a server whose address is "www.mit.edu"). So you know you have indeed connected to the server you have intended to reach.
2) Verifies that the person who requested the certificate is a duly authorized representative of the entity named on the certificate (e.g. someone from stamford.edu cannot obtain a certificate for mit.edu)
3) Encrypts communication between the server and the client browser.
4) Allows only authorized individuals (with the correct certificate installed in their client browser) to connect to the web server

The encryption portion of the certificate's job is accomplished regardless of what kind of certificate is installed on the server. The verification portion (#2 above), however, requires a **Certification Authority (CA)** – an organization whose job it is to ensure that someone who requests a certificate for an organization is authorized to do so. The Certification Authority creates the actual certificate and returns it to the requestor for installation on a web site.

Roughly speaking, there are three types of Certification Authorities:

1) Public Certificate Authorities, such as VeriSign
2) Large private Certificate Authorities, such as MIT
3) Small private Certificate Authorities, such as your own Certificate Server [1]

If using a public or large private CA, you must create a certificate request and send it to the CA. The CA will probably request information from you verifying your identity and your authority to act on behalf of your institution. This process can potentially take several weeks. If you are using your own Certificate Server, you can process your certificate immediately.

It should be noted that most browsers include the public keys of the major public Certification Authorities. In Internet Explorer, select Tools->Internet Options->Content->Publishers->Trusted Root Certification Authorities to see the list of certificates that are included in IE.

Most browsers will pop up a notice if there is a problem with the server certificate, but will allow you to proceed nevertheless. Problems that might be reported are:

- “Certificate was issued by a company you have not chosen to trust.” This means the CA’s certificate is not in your Trusted Root Certification Store. You should have the option of installing the certificate. An example of a site which might cause this message to appear is MIT, which has its own Certificate Authority but whose certificate is not included in browsers by default.
- “The security certificate has expired or is not yet valid.” Certificates have expiration dates.
- “The name on the security certificate is invalid or does not match the name of the site”. This means that the host is not the named owner of the certificate (e.g., a certificate designated for “abc.com” has been installed on a server at “xyz.com”; or, more commonly, a certificate for “www.abc.com” is installed on “xyz.abc.com”).

[1] If you wish, you can install Microsoft Certificate Server on your machine, and issue your own certificates. Go to Start->Control Panel->Add or Remove Programs -> Add/Remove Windows Components. Check the Certificate Services box and complete the Wizard.

Securing the Web Server

This section covers the steps involved in obtaining and installing a certificate on your server. Once the certificate is installed, users will be able to log in to the Service Broker over a secure connection (https).

It should be noted that the Service Broker does not require the use of SSL; if you do not intend to use SSL, please skip this section. Using SSL assumes that you will purchase a certificate from a Certificate Authority (such as Verisign) or run your own certificate authority.

Also, it should be noted that if you are planning to develop code using Visual Studio you should not use SSL on your development Service Broker. Visual Studio does not handle SSL connections.

To begin, open the Microsoft Management Console for IIS:

- ❑ Right-Click on **My Computer** (renamed to your computer name)
- ❑ Click **Manage**
- ❑ Expand **Services and Applications**
- ❑ Expand **Internet Information Services**
- ❑ Expand **Web Sites**
- ❑ Right-click **Default Web Site**
- ❑ Select **Properties**
- ❑ **Directory Security** tab
- ❑ Click the **Server Certificate** button in the “Secure Communications” box at the bottom
- ❑ The Web Server Certificate Wizard starts. You should see a message that says “Your web server doesn’t have a certificate installed and you don’t have any pending requests”. Click **Next ->**
- ❑ Select **Create a New Certificate**, and click **Next ->**
- ❑ Select **Prepare the request now, but send it later** and click **Next->**
- ❑ Type a name for the new certificate. Use the fully qualified domain name, e.g. server.yourschool.edu. Leave the other defaults, and click **Next ->**
- ❑ Fill in the organization and organizational unit names, and click Next ->
- ❑ Type the common name. This is the fully qualified domain name, e.g. server.yourschool.edu.
- ❑ Fill in your country, state, and city
- ❑ Fill in a name for the certification request file (leave the default of c:\certreq.txt). Click **Next ->**
- ❑ Review the Request File Summary, and click **Next ->**
- ❑ Click **Finish**

The next step in the process is to send the Certificate Request (certreq.txt) to a Certification Authority, which will use it to generate a certificate for your server. If you are using a public Certification Authority such as VeriSign, you will need to send them an email with c:\certreq.txt attached. If you are using your own instance of Microsoft Certificate Server, you will paste the contents of certreq.txt into a web form on the machine where Certificate Server is running. Whichever process you use, the end result is that you should receive a certificate file with a .cer extension from the Certificate Authority, which will become your web server's certificate.

Import the certificate as follows.

- Return to the **Directory Security** tab in IIS (see above)
- Click the **Server Certificate** button in the "Secure Communications" box at the bottom
- The Web Server Certificate Wizard starts. You should see a message that says "You have a pending certificate request". Click **Next ->**
- Select **Process the pending request and install the certificate** , and click **Next ->**
- Browse to the location of your certificate file. It should end in a .cer extension. When you have located it, click Open, the click Next ->
- For SSL port, leave the default of **443**, and click **Next ->**
- Review the Certificate Summary, and click **Next ->**
- Click **Finish**
- Click **OK** to close the Web Site Properties page.

At this point, you should be able to access your web site securely using https://yourserver.yoursite.edu. *Note: Make sure you have opened the firewall on port 443 before you try to connect.*

Configuring the Service Broker for SSL

If you are running a secure Service Broker, you must make some changes to web.config. Under <configuration><appSettings>, set the following keys:

```
<add key="haveSSL" value="true" />
<add key="secureProtocol" value="https" />
```

Note: If your Service Broker does not have a certificate installed, the site will not function if you are configured to use SSL in web.config.

Testing Your SSL Installation

- Open Internet Explorer
- Browse to https://localhost/ServiceBroker
- Log in as follows:
    - Username: **superUser**
    - Password: **ilab**

For information on how to configure a Service Broker to work with a sample lab, please see ***Time of Day Sample Lab Server.doc***.

Communicating with a Secure Lab Server

Some lab servers, notably the Microelectronics WebLab Lab Server at MIT, require the Service Broker to communicate over SSL. The WebLab server uses a certificate issued by the MIT Certification Authority, which is not by default trusted by commonly available web browsers. This is not a problem if a user is browsing a web site, as the browser will present the user with a pop-up informing them that this is not a trusted certificate, but allowing them to proceed nevertheless.

The Service Broker communicates using Web Services, which, unlike a browser, are unable to negotiate a connection with a non-trusted secure web server unless hard-coded to do so. Therefore, if your Service Broker needs to make a secure connection with a machine whose certificate has been issued from a non-public Certification Authority, you will need to install that CA's certificate on your Service Broker.

Following are the steps necessary to obtain and install MIT's certificate. You can use these same steps to install the certificate from any other CA, as well.

- ❑ Go to http://web.mit.edu/is/topics/certificates/
- ❑ Under **Get Certificates Now**, click on **Get MIT CA (Certificate Authority)**
- ❑ Save the file **mitca.cer** to your hard drive
- ❑ Create a Certificate Microsoft Management Console (MMC) Snap-in. **Start->Run…mmc**
- ❑ **File->Add/Remove Snap-In**
- ❑ Click the **Add…** button
- ❑ Select **Certificates**
- ❑ Click the **Add…** button
- ❑ Select **Computer account**
- ❑ Click **Next>**
- ❑ Select **Local Computer**
- ❑ Click **Finish**
- ❑ Click **Close**
- ❑ Click **OK**
- ❑ Expand **Certificates (Local Computer)**
- ❑ Right-click **Trusted Root Certification Authorities**
- ❑ **All Tasks->Import…**
- ❑ **Next>**
- ❑ **Browse** to the location where you saved **mitca.cer**
- ❑ Select **mitca.cer**, and click **Open**

- ❑ **Next>**
- ❑ Make sure **Place all certificates in the following store** is selected, and that **Trusted Root Certification Authorities** appears in the box. If it does not, click the **Browse** button and correct it.
- ❑ **Next>**
- ❑ **Finish**
- ❑ **OK**
- ❑ The Certificates console is a handy thing to keep on your machine. To save it so that you can open it without having to add the Certificate snap-in again, click **File->Save As**, type **Certificates.msc** in the box, and click **Save**. It should now appear as an option in **Start->All Programs->Administrative Tools**
- ❑ Close the Certificate MMC Console.
- ❑ Reboot the machine

Visual Studio.NET 2003

Product Installation

Note: If this machine is not going to be used for development, installation of Visual Studio.NET is not necessary.

This is a lengthy process.

- ❑ Right-click on **My Computer** and click on **Manage**.
- ❑ Expand **Local Users and Groups**
- ❑ Double-click on **Users**
- ❑ Right-click on **Administrator**
- ❑ Click **Set Password.**
- ❑ Type a password twice, and click **OK**
- ❑ The password has been changed. Click **OK**
- ❑ Close the Computer Management window.

Now get the Visual Studio.NET 2003 CDs. There should be three at a minimum, seven for the full installation:

1) Visual Studio.NET 2003 Prerequisites
2) Visual Studio.NET 2003 Enterprise Architect, Disc 1
3) Visual Studio.NET 2003 Enterprise Architect, Disc 2
4) Visual Studio.NET 2003 Library, Disc 1
5) Visual Studio.NET 2003 Library, Disc 2
6) Visual Studio.NET 2003 Library, Disc 3
7) Visual Source Safe 6.0d (Optional; install if you want to have a source control environment on this machine)

- ❑ Insert Visual Studio.NET 2003 Enterprise Architect, Disc 1. Wait a moment for Autorun to start.
- ❑ Click on **Visual Studio.NET Prerequisites**.
- ❑ When prompted, Insert Visual Studio.NET 2003 Prerequisites. Click **OK** when ready.
- ❑ License agreement: Click **I agree**.
- ❑ Click **Continue**
- ❑ Click **Install Now**.
- ❑ Check box next to **Automatically log on**. Enter your Administrator password twice.
- ❑ Click **Install Now!**
- ❑ When the Prerequisites Installation finishes (it will take a few minutes, click **Done**.
- ❑ Click **2. Visual Studio.NET**
- ❑ When prompted, insert Visual Studio.NET Disk 1. Click **OK** when ready.
- ❑ License Agreement: Click **I agree**
- ❑ Type in the machine name next to **Your Name**
- ❑ Click **Continue**
- ❑ Accept the defaults, and click **Install Now!**
- ❑ Insert Visual Studio.NET Disk 2 when prompted (After approx. 15 minutes). Click **OK**
- ❑ After approx. 15 minutes, you will see this message: **Step 2 of Setup is complete**. Click **Done**. Remove the CD.
- ❑ Click **3 - Product Documentation**
- ❑ When prompted, insert Visual Studio Library Disk 1 (prompt might specify MSDN disk 1). Click **OK.**
- ❑ Welcome… Click **Next>**
- ❑ License Agreement: Check **I accept** the terms…
- ❑ Click **Next->**
- ❑ Enter the machine name for User Name, and MIT for the Organization.
- ❑ Click **Next->**
- ❑ Check **Full**
- ❑ Click **Next->**
- ❑ Accept the default destination folder, and click **Next->**
- ❑ Click **Install**
- ❑ When prompted, insert Visual Studio Library Disk 2. Click **OK.**
- ❑ When prompted, insert Visual Studio Library Disk 3. Click **OK.**
- ❑ Library Setup Wizard Completed. Click **Finish**
- ❑ Click **Exit**
- ❑ Security Updates: Click **No** (we'll do this later)

iLabs Project

Now, create the Visual Studio project. Note: This step is not necessary if you do not intend to develop on this machine.

- ❑ Start->Run->Microsoft Visual Studio.NET 2003-> **Microsoft Visual Studio.NET 2003**
- ❑ Click on the **Projects** tab
- ❑ Click **Open Project**
- ❑ Browse to **D:\MIT iCampus\iLabs\serviceBroker60\architecture\ILabs.sln**
- ❑ Click **OK**
- ❑ Wait while Visual Studio loads the code. If you get an error message that says that it cannot find the directory, simply correct it by browsing to the location where the code in question currently resides.
- ❑ Do a Test Build: **Build->Build Solution**. If it builds without errors, your installation is a success

Note: You cannot develop in Visual Studio against a website that is running SSL. If you have problems, check to make sure that SSL is not turned on in web.config. See **Configuring the Service Broker for SSL** on p. 22.