GERENJISUANJI
ANQUANFANGHUZHINAN

个人计算机安全防护指南

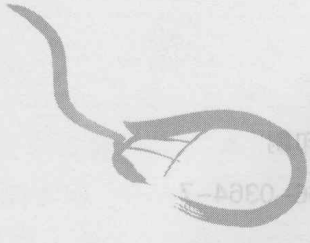
编委会主任　吕家国
主　　编　李桂玲
副 主 编　赵新青　杨永丽

这里我们想给出用户一个高效、安全使用计算机的操作使用方案，
按照这一方案配置使用我们的计算机会使计算机速度更快，
全性能更高。我们给出的操作使用方案是把计算机操作系统本身原
有的功能进行组合、解释。
让用户知道为什么用，怎么用！

河北大学出版社

个人计算机安全防护指南

编委会主任：吕家国
主　　编：李桂玲
副 主 编：赵新青　杨永丽
编　　委：黄　亮　宋志远　臧建莲
雷武龙　李艳静



河北大学出版社

个人计算机安全防护指南

图书在版编目（CIP）数据

个人计算机安全防护指南 / 李桂玲主编. — 保定 : 河北大学出版社, 2013.3

ISBN 978-7-5666-0364-7

Ⅰ. ①个… Ⅱ. ①李… Ⅲ个人计算机－安全技术－指南 Ⅳ. ①TP368.309-62

中国版本图书馆CIP数据核字(2013)第040555号

GERENJISUANJI ANQUAN FANGHUZHINAN

责任编辑：杨显硕

装帧设计：赵　谦

责任印制：靳云飞

出版：河北大学出版社

地址：河北省保定市五四东路180号

经销：全国新华书店

印刷：保定市北方胶印有限公司

开本：1／16（787mm×1092mm）

字数：150千字

印张：7.5

版次：2013年5月第1版

印次：2013年5月第1次印刷

书号：ISBN 978-7-5666-0364-7

定价：16.00元

前　言

网络技术的飞速发展，令公众始料不及。网络已深入到人们生活的各个方面，正在不断改变着人们的工作生活方式，然而，IP 网络是一把双刃剑。IP 网络的共享性、开放性在给信息技术的发展带来革命性变革的同时，各种病毒、木马以及非法的网络访问等行为，正在威胁着计算机网络的安全，各类计算机用户都不同程度地处在危险当中。

本书的作者长期从事计算机网络安全工作，熟悉计算机网络的建设、管理特点与安全现状，在日常工作中经常为用户解决各类计算机网络安全问题，积累了大量的实践经验。我们总结了一些有关计算机终端安全设置的操作方法，在工作之余，把它编撰成册，供大家查阅参考。

本书共分为安全基础知识、基础篇、高级篇和其他安全手段介绍四部分。安全基础知识主要讲解了计算机安全的基本概念；基础篇主要从安全角度讲解了操作系统的安装、备份等基本操作，以及计算机最低限度安全防护手段的使用配置；高级篇讲解了计算机操作系统安全加固等较深层次的安全配置方法；其他安全手段介绍部分讲解了一些保护计算机安全的其他方法。

由于编者水平有限，虽尽了最大努力，但书中难免有错漏之处，欢迎读者批评指正。

编者

2013 年 4 月

目 录

第Ⅰ部分　安全基础知识

第1章　安全基础知识

1.1　什么是计算机安全

“安全”是指“远离危险、威胁的状态或特性”。计算机安全是指计算机系统的硬件、软件、数据受到保护，不因偶然的或恶意的原因而遭到破坏、更改和泄露，系统能连续正常运行。从技术上讲，计算机安全分为三种：

1. 实体的安全性

它用来保证硬件和软件本身的安全。

2. 运行环境的安全性

它用来保证计算机能在良好的环境中持续工作。

3. 信息的安全性

它用来保障信息不会被非法阅读、修改和泄露。

也有人认为，根据计算机系统组成的层次结构，计算机安全应包括硬件及其运行环境（温度、湿度、灰尘、腐蚀、电气与电磁干扰）安全、操作系统安全、数据库安全和应用软件安全等四部分。

计算机安全具有三个方面的特性，即保密性、完整性和可用性。这三个技术特性也反映了计算机系统的安全需求。

1. 保密性

保密性是指计算机系统能够防止非法泄露计算机数据。

2. 完整性

完整性是指计算机系统能够防止非法修改或删除数据和程序。

3. 可用性

可用性是指计算机系统能够防止非法独占资源，并能为用户提供及时的和持续的服务。

1.2　什么是 CMOS

“CMOS”是指计算机内一个保存计算机基本启动信息（如日期、时间、启动设置等）的电脑芯片，由于系统的开机密码及进入 CMOS 的密码保存在该芯片内，所以设置开机密码及 CMOS 的密码也叫做设置 CMOS 密码。

1.3　什么是注册表

注册表是管理计算机资源的数据库，用于存储系统和应用程序的设置信息。例如上网

的 IP 地址、启动程序、安装的软件等等都在注册表里面保存着。安装应用程序时经常会提示是否允许修改注册表，许多病毒程序、黑客程序也都需要修改注册表添加启动项达到自动运行病毒和黑客程序的目的，因此注册表对计算机系统及用户来说非常重要。

1.4 什么是服务

计算机完成的某一特定的功能，就称为计算机提供的一种服务。服务可以根据用户的需要进行开启或关闭。

1.5 什么是组策略

组策略是计算机提供给用户的一个编辑修改计算机注册表某些项的实用程序。它比用注册表编辑器修改注册表更加方便。

1.6 什么是 TCP/IP 协议

通俗的讲，协议就是双方或多方之间需要共同遵守规定或条款，同样，计算机之间要相互通信，事先要规定一些通信规则，双方按照规则发送信息才能互相明白通信内容代表的含义，双方需要遵守的这些规定或规则就是所谓的通信协议。在计算机网络中，TCP/IP 协议(Transmussion Control Protocol/Internet Protocol)是传输控制协议和网际互联协议的缩写。

IP 协议负责数据的传输，TCP 协议则负责数据的可靠性。

1.7 什么是端口及端口号

我们可以把计算机的“端口”理解为其他计算机与之联系的通道，每个计算机有许多类似的通道，这些通道通过一定的手段就可以相互勾通联络。

更深入的讲，计算机的端口一般是指 TCP/IP 协议中的端口，在 TCP/IP 协议中，每台主机可以同时完成多个网络通信请求，为了区分这些请求，使其相互之间不受影响，为每个请求分配一个标识(号码)。这种标识用“IP 地址:端口号(端口号的范围从 0 到 65535)”的形式来表示。例如:某计算机的 IP 地址为 218.25.228.18，若这台计算机同时启动了三个 QQ 进程，那么第一个 QQ 的地址用 218.25.228.18:4000 表示，第二个 QQ 的地址用 218.25.228.18:4001;表示;第三个 QQ 的地址用 218.25.228.18:4002 表示，这样三个 QQ 和外界通信时就不互相干扰了。

1 知名端口(Well－Known Ports)

知名端口即众所周知的端口号，范围从 0 到 1023，这些端口号一般固定分配给一些服务。比如 21 端口分配给 FTP 服务，25 端口分配给 SMTP(简单邮件传输协议)服务，80 端口分配给 HTTP 服务，135 端口分配给 RPC(远程过程调用)服务等等。

2 动态端口(Dynamic Ports)

动态端口的范围从 1024 到 65535，这些端口号一般不固定分配给某个服务，也就是说许多服务都可以使用这些端口。只要运行的程序向系统提出访问网络的申请，那么系统就可以从这些端口号中分配一个供该程序使用。比如 1024 端口就是分配给第一个向系统发出申请的程序。在关闭程序进程后，就会释放所占用的端口号。

由于计算机的端口都是公开的，因此，病毒和木马经常利用这些通道侵入计算机。因此有必要关闭一些通道，以防止病毒和木马的入侵。

1.8　什么是 Cookies

Cookies 亦称 Cookie。

Cookies 是一种能够让网站服务器把少量数据储存到客户端的硬盘或内存，或是从客户端的硬盘读取数据的一种技术。Cookies 是当你浏览某网站时，由 Web 服务器置于你硬盘上的一个非常小的文本文件，这个小的文本文件就是 Cookies。它可以记录你的用户 ID、密码、浏览过的网页、停留的时间等信息。当你再次来到该网站时，网站通过读取 Cookies，得知你的相关信息，就可以做出相应的动作，如在页面显示欢迎你的标语，或者让你不用输入 ID、密码就直接登录等等。

从本质上讲，Cookies 可以看做是你的身份证。Cookies 中的内容大多数经过了简单的加密处理，但利用一些专门查看 Cookies 的软件，可以看到 Cookies 的内容，因此在使用 Cookies 也是一种潜在的危险。

第Ⅱ部分　基础篇

第2章　系统的安装

2.1　系统安装、备份和恢复

我们买回一台新电脑，电脑里面操作系统是事先安装好的，一般来说这款操作系统是比较完整的，它会根据你的电脑硬件配置把各种驱动程序安装完整，并且把各种常用的应用程序安装完毕。一般情况下用户很少去重新安装操作系统，但是，如果你的电脑使用一段时间以后，计算机内安装的软件越来越多，安装的软件越来越大，经常删除和重新安装大的游戏软件，此时会感觉到计算机开机速度变慢，启动各种应用程序的速度也变慢，这是因为系统内部残留了很多“垃圾”。这不是计算机本身性能的下降，而是计算机的资源被占用和浪费了。此时比较有效的方法是重新安装一次操作系统，会使计算机的运行速度恢复正常。但是计算机内已安装的各种应用程序就需要重新安装，非常烦琐，所以应采取的策略是在系统运行良好时做好系统备份，必要时将操作系统恢复到备份前的状态。

当然如果电脑发生软件故障，无法正常启动，也许就需要重新安装操作系统，这时我们有二个选择，使用安装版或 Ghost 版的操作系统，它们有什么不同呢？

2.2　安装版与 Ghost 版的区别

安装版就是该版本的安装是按照微软公司原版 Windows 的安装步骤，分区、格式化、复制文件、安装等一步步进行的。优点是稳定性、兼容性高，适合所有硬件平台，缺点是安装步骤多、耗费时间长。安装版并不一定就是原版，也可以是经过剪裁的修改版。

Ghost 版是采用赛门铁克的 Ghost 软件对系统进行打包，然后用 Ghost 软件释放打包系统的一种快速安装系统。它是在原版系统基础上去掉部分 Windows 组件、修改部分系统信息、安装第三方应用程序、增加大量硬件驱动程序以适应不同硬件平台的系统。由于 Ghost 版的作者为了精简去掉了一些组件，用户在使用过程中可能遇到很多专业软件无法使用，部分硬件驱动无法安装，系统设置不能够修改的现象，导致了系统在使用过程中的稳定性、兼容性大打折扣，影响用户正常使用，且有的作者为了私人利益会在封装前在系统中植入木马、病毒等，给用户电脑带来安全风险。但由于 Ghost 版系统有着装机速度快、包含大量第三方驱动和常用软件等优点，为许多人所喜爱。

作为普通用户，如果对系统稳定性、兼容性没有过高要求，可以在众多 Ghost 版系统中选择技术水平高、口碑好的，如深度、番茄花园等。下面就以 Win XP 系统为例，介绍安装版和 Ghost 版的安装过程。

2.3　在 BIOS 中设置光盘启动

计算机系统的一些基础程序、设置（包括开机密码）被称为“基本输入输出系统”即

BIOS，保存在计算机内一个叫做“CMOS”的电脑芯片内，所以有人常常把 BIOS 设置称为 CMOS 设置。它们的区别在于前者指的是程序，是软件；后者指的是载体，是硬件，本文中对二者不作区分。

安装系统时一般需要使用光盘启动，设置 BIOS 主要是设置系统的引导顺序，即系统是从硬盘、光驱、U 盘还是从网络等其他设备引导。一般台式机按 DEL(Delete)键可进 BIOS 设置，而笔记本由于品牌众多，进入 BIOS 的方法都有区别，比如：联想(Lenovo)一般是按 F2，惠普(HP)可按 Esc 进入 BIOS，一般可查看开机 Logo 的提示。图 2－3－1 是某型机的开机画面，从图中可以看出，按 DEL 键进入 BIOS，按 F11 键进入引导菜单。

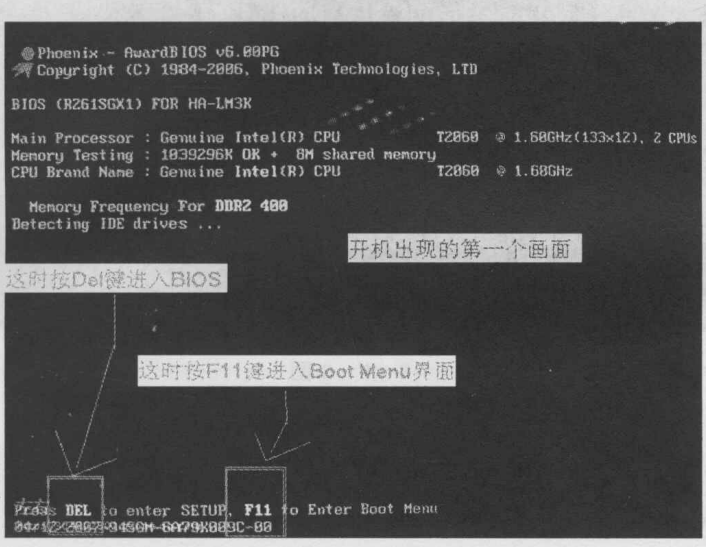


图 2－3－1　开机画面

按 DEL 键后，系统进入 BIOS 程序，在 Boot 菜单中，按“＋”键将电脑设置为首先从 CD－ROM光驱启动，按 F10 保存并自动重启电脑，如图 2－3－2 所示。

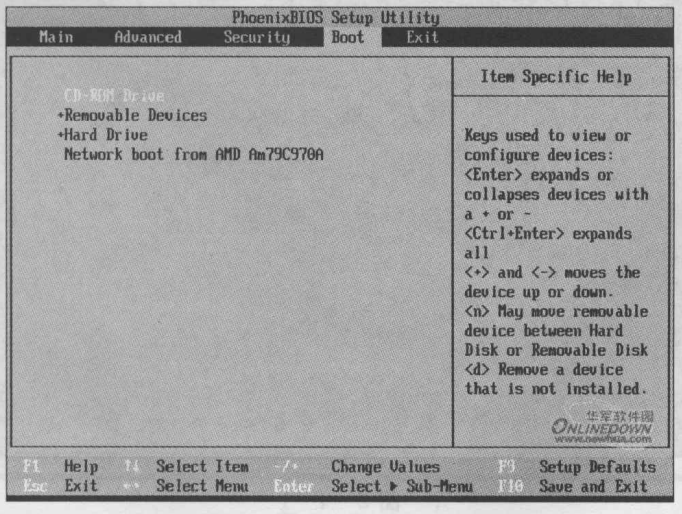


图 2－3－2　BIOS 引导顺序设置

上面的方法改变了 BIOS 设置，如果只是临时性的光盘引导，可在图 2－3－1 中按 F11 键，将显示引导菜单如图 2－3－3 所示，用于设置本次的引导顺序，图中选择 DVD/CD－ROM，本次从光盘引导，下次启动时仍按 BIOS 中设置的顺序进行。

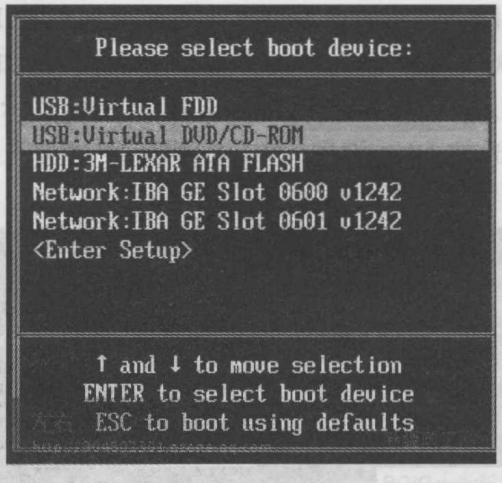


图 2－3－3　Boot Menu 界面

2.4　XP 安装版安装

电脑启动后将自动从光驱加载 Windows XP 的安装程序，开始进行安装。图 2－4－1 显示了初始画面，按回车键继续。

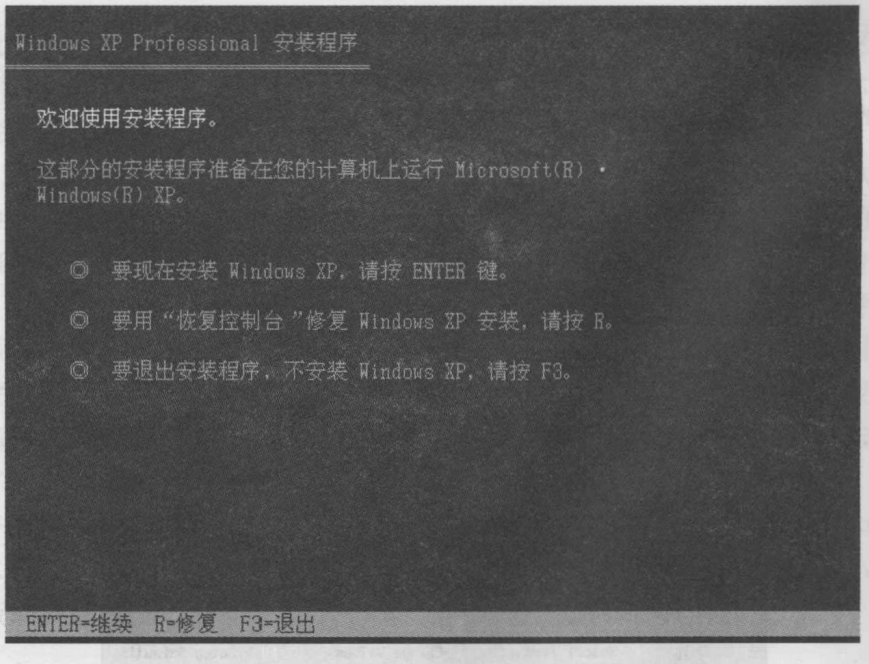


图 2－4－1

出现图 2—4—2 后，按 F8 同意继续。

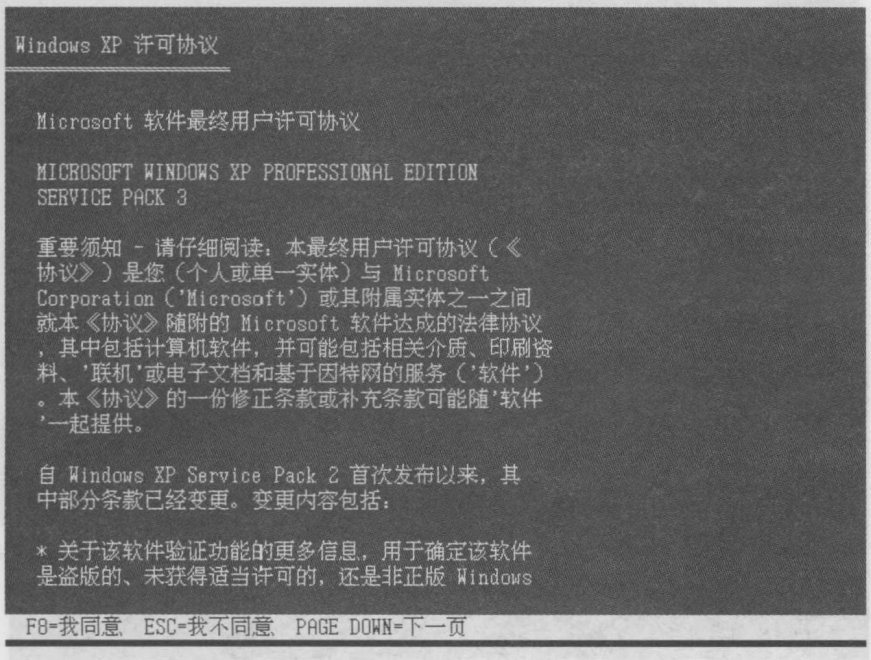


图 2—4—2

未安装过系统的电脑其磁盘分区如图 2—4—3 所示，按 C 键创建磁盘分区，分区大小一般为磁盘总容量的四分之一左右，也可直接使用整个硬盘，装完系统后再根据需要调整分区大小。

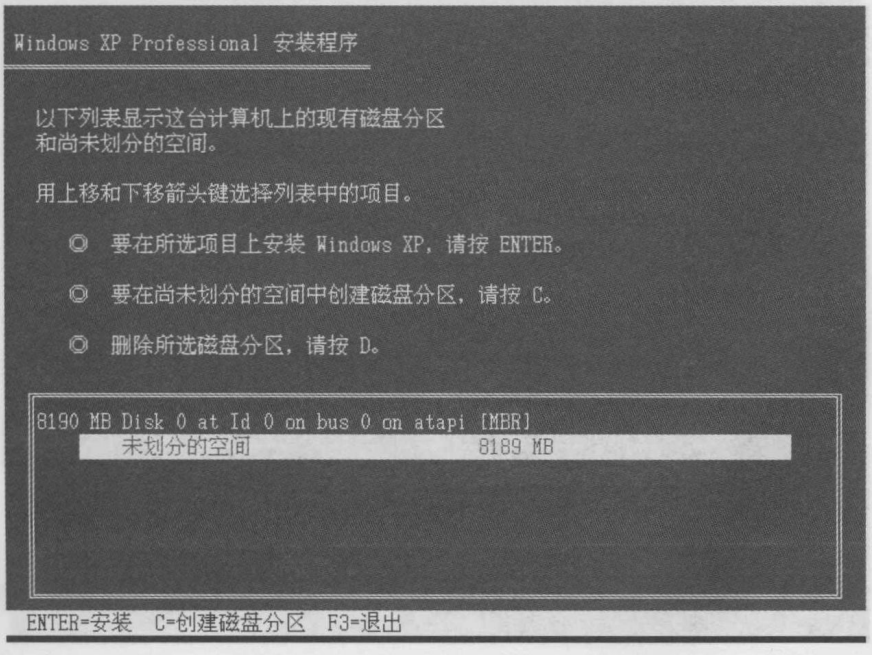


图 2—4—3

建议使用 NTFS 文件系统格式化分区，这样文件系统的效率和安全性更高，如图 2－4－4所示。

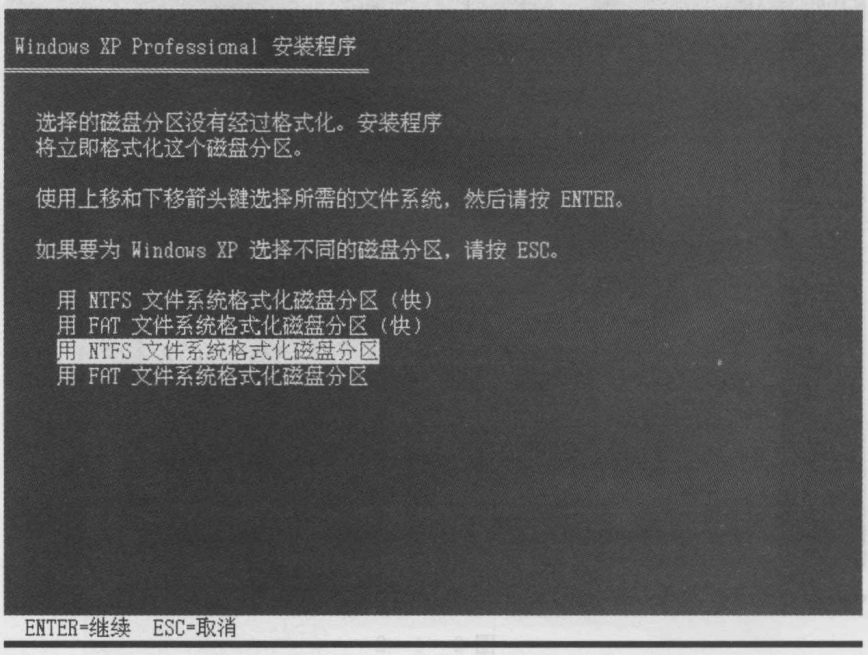


图 2－4－4

图 2－4－5 显示了正在进行格式化，磁盘格式化完毕，系统开始复制安装系统所需文件，如图 2－4－6 所示。

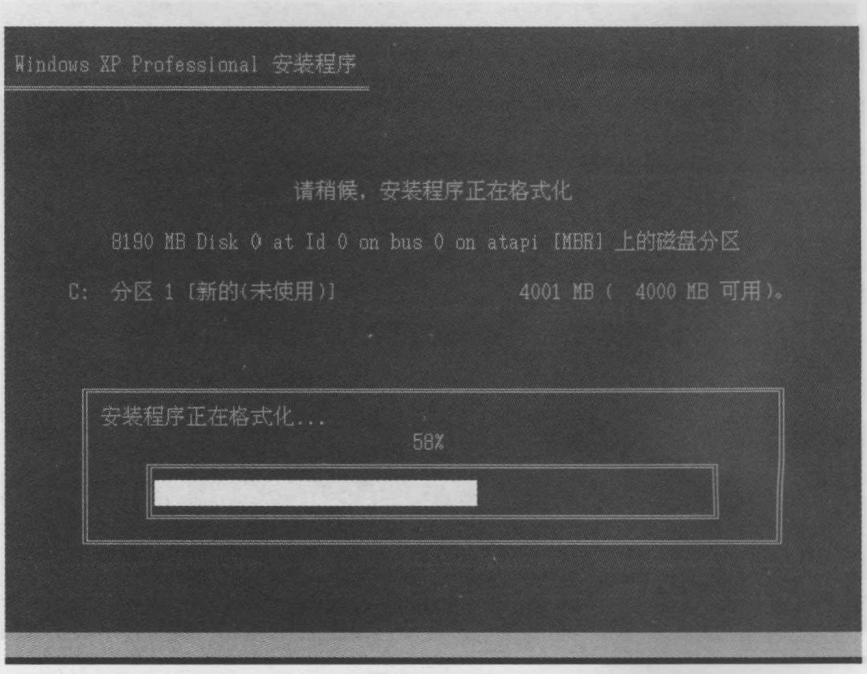


图 2－4－5

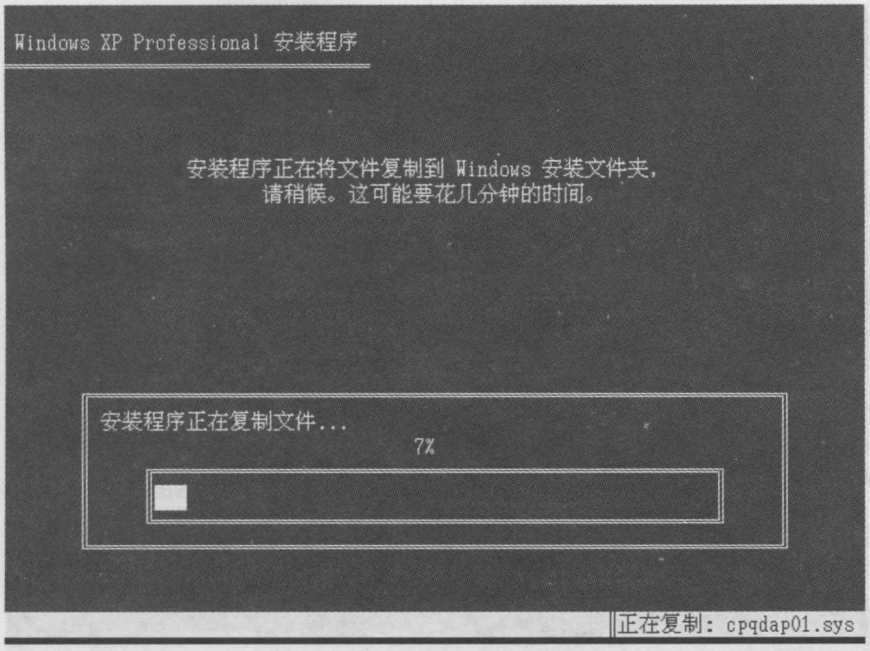


图 2－4－6

文件复制结束后，电脑会自动重启，进入安装阶段，如图 2－4－7 所示。

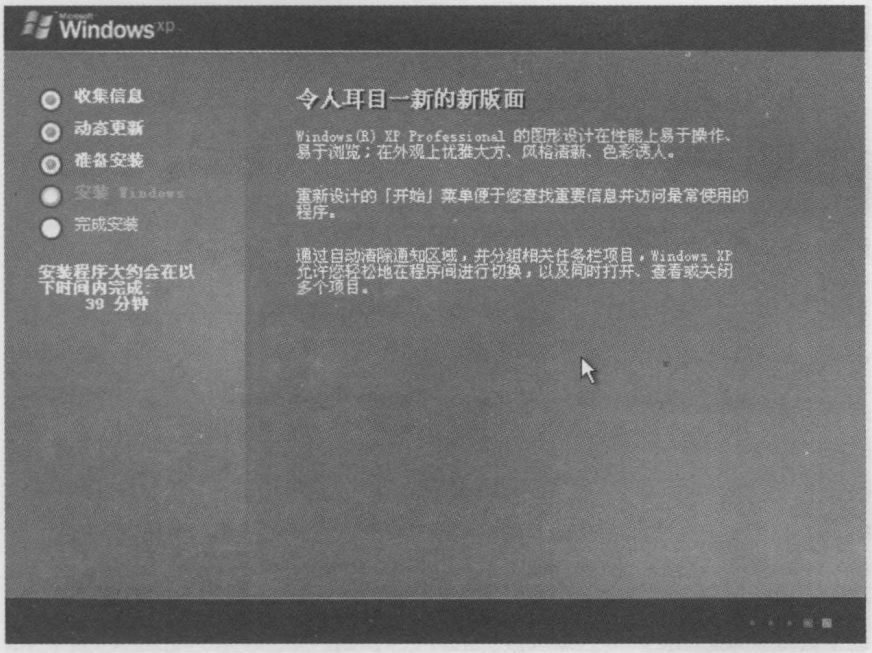


图 2－4－7

系统安装过程中，要求用户对系统进行初始化设置，一般使用默认。

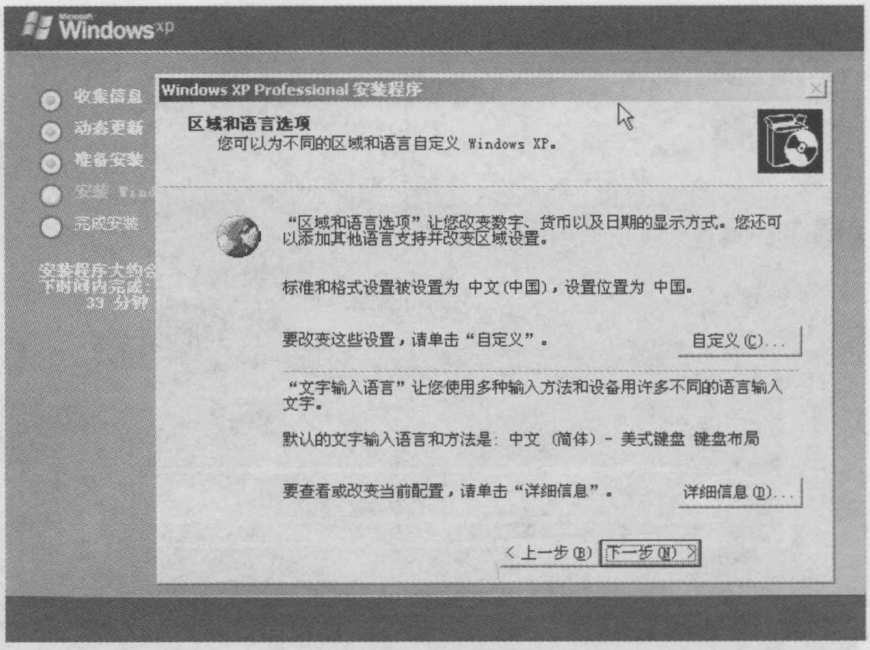


图 2－4－8

填写用户姓名，单位。

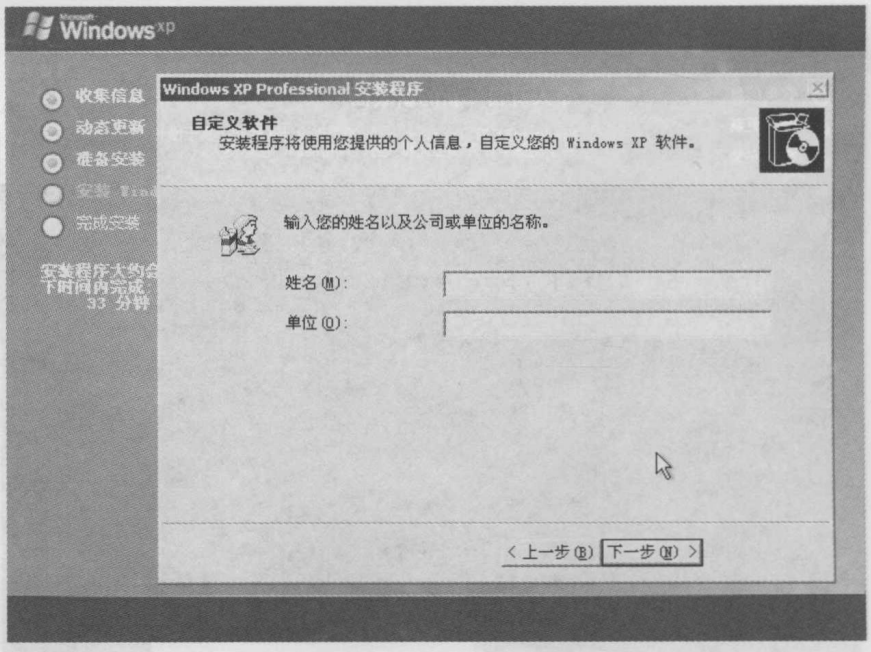


图 2－4－9

输入相应序列号。

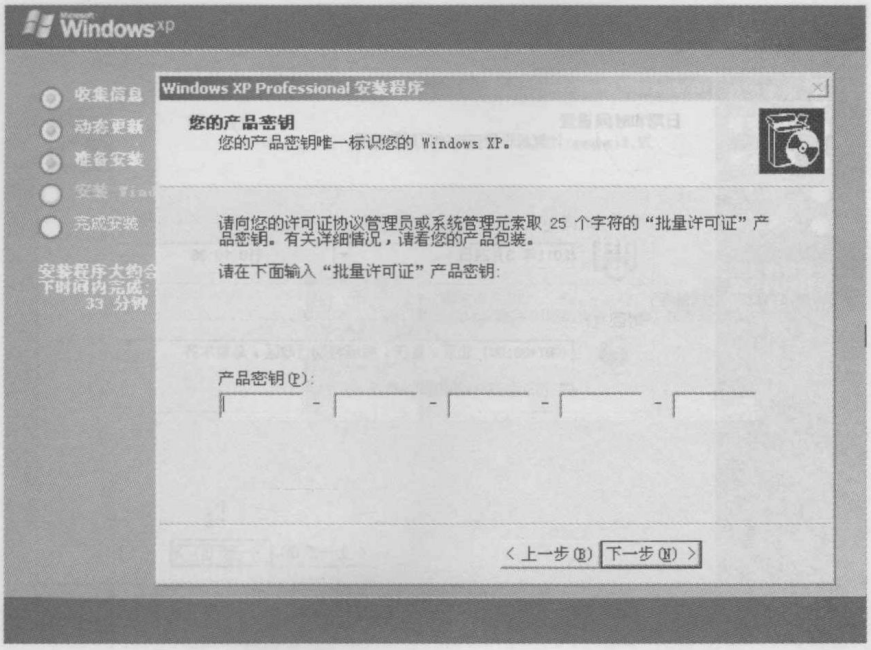


图 2－4－10

设置超级管理员密码，建议使用 8 位以上数字和字母混合。

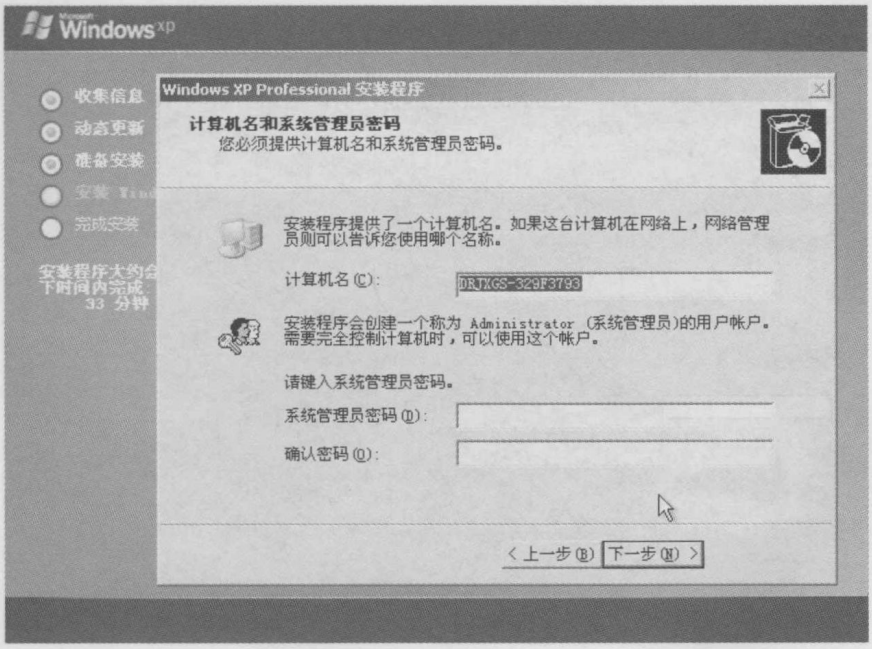


图 2－4－11

设置时间，默认即可。