在获取了一些经验后，代码标注也不那么令人满意了，所以安全模式又有了变化。JDK 1.2版本提供了一套可配置的严密的安全策略，针对包含本地和异地所有的Applet。安全模式非常复杂导致需要整整一本书来描述（Gong, 1999），我们仅仅归纳出一些精华的部分。

每一个Applet具有两个特性：来源于何处以及谁签署了它。来源于何处是指URL，谁签署了它是指签名所用的私钥。每个用户都能创建包含规则列表的安全策略。规则列出了URL、签署者、对象以及如果Applet的URL和签署者匹配规则时可在对象上执行的动作。从概念上来说，上述信息如图9-39所示，虽然真正的格式有所不同并且与Java的类等级有关。

URL	签署者	对象	动作
www.taxprep.com	TaxPrep	/usr/susan/1040.xls	Read
*		/usr/tmp/*	Read, Write
www.microsoft.com	Microsoft	/usr/susan/Office/–	Read, Write, Delete

图9-39 JDK 1.2所指定的某些保护规则的实例

其中的一种允许的动作是访问文件。该动作可以指定某一特定的文件或目录，给定目录下的所有文件，或给定目录下所有的文件和子目录的递归集合。图9-21的三行包含了3种情况。在第一行里，用户Susan建立了她的许可文件，这样来自她的税务预备用计算机，www.taxprep.com，并由该公司签名的Applet可以访问位于1040.xls文件里的她的税务数据。这是惟一可读的文件，并且任何其他的Applet都不能读。而且，来自于所有资源的所有Applet，无论是否签名，都可以读写/usr/tmp中的文件。

而且，Susan也信任Microsoft，让来自于该公司站点并签名过的Applet读、写或删除Office目录下的所有文件。例如，修复bug并安装新的软件版本。为了校验签名，Susan要么在她的磁盘里存放公钥，要么动态地获取公钥，例如，在持有她所信任的公司的公钥以后，使用该公司的签名证书格式。

文件不是仅仅要保护的资源。网络访问也可以被保护。被保护的对象是特定计算机的特定端口。每一台计算机由一个IP地址或DNS名确定；计算机上的端口由一排数字确定。可能的动作包括要求连接远程计算机以及接受来自远程计算机的连接。通过这种方法，Applet可以获得访问网络的权限，但仅局限于与许可列表中明示的计算机进行交谈。Applet可以动态地装入所需的附加代码（类），但用户提供的类装载器可以精确地控制由哪台计算机产生这样的类。当然还有其他大量的安全特性。

9.9 有关安全性研究

计算机安全性是一个非常热门的话题，很多人都在研究。其中一个重要的话题就是可信计算，尤其是可信计算的平台（Erickson，2003；Garfinkel等人，2003；Reid和Caelli，2005以及Thibadeau，2006）和相关的公共政策话题（Anderson，2003）。信息流的模型和实现是一个正在研究的话题（Castro等人，2006；Efstathopoulos等人，2005；Hicks等人，2007和Zeldovich 等人，2006）。

用户验证（包括生物学识别）仍然是很重要的（BhargavSpantzel 等人，2006；Bergadano 等人，2002；Pusara和Brodley，2004；Sasse，2007 以及Yoon 等人，2004）。

各种恶意软件被广泛地研究，包括特洛伊木马（Agrawal 等人，2007；Franz，2007和Moffie等人，2006）、病毒（Bruschi 等人，2007；Cheng 等人，2007和Rieback 等人，2006）、蠕虫（Abdelhafez 等人，2007；Jiang和Xu，2006；Kienzle和Elder，2003以及Tang和Cheng，2007）、间谍软件（Egele 等人，2007；Felten和Halderman，2006以及Wu 等人，2006）和rootkit（Kruegel 等人，2004；Levine 等人，2006；Quynh和Takefuji，2007以及Wang和Dasgupta，2007）。既然病毒、间谍软件和rootkit都会尽力地隐藏，那么就会有关于stealth技术的工作以及它们怎么样才能被侦测到（Carpenter 等人，2007；Garfinkel 等人，2007以及Lyda和Hamrock，2007）。加密技术本身也要被检查（Harmsen和Pearlman，2005以及Kratzer 等人，2006）。

9.10 小结

计算机中经常会包含有价值的机密数据，包括纳税申请单、信用卡账号、商业计划、交易秘密等。这些计算机的主人通常非常渴望保证这些数据是私人所有，不会被窜改，这就迅速地导致了我们要求操