DOI: 10.3969/j.issn.1672-8874.2009.01.035

信息安全保密课堂教学方法的创新设计*

何鸿君, 罗 莉, 任江春, 彭立宏, 王学惠
(国防科学技术大学 计算机学院, 湖南 长沙 410073)

[摘 要] 为提高信息安全保密教学效果, 需要采取多种教学手段。计算机文件删除操作存在安全隐患, 文件被恢复之后造成泄密是一种重要的泄密渠道。针对此问题, 采取“欲擒故纵”式教学手法, 能迅速吸引学生目光, 引导其展开深入思考, 收到了良好效果。

[关键词] 教学效果; 信息安全保密; 欲擒故纵; 教学手法
[中图分类号] G642.4 [文献标识码] A [文章编号] 1672-8874(2009)01-0099-02

信息安全保密是当前大学教育的一项重要内容, 掌握基本的保密、窃密知识和技能是现代大学生的必备素质。但由于大学生的经常性教育中宣灌式教育成分较重, 对于信息安全保密的课堂教学, 学生容易产生逆反情绪, 根本就不在乎听课, 考前临时抱佛脚, 考完以后很快就还给老师了。为达到好的教学效果, 需要迅速抓住学生的注意力。为此, 我们采取“欲擒故纵”式教学方法, 设计一个不经意的失误, 把学生的焦点一下子落在老师身上。然后, 再采取师生互动的方式, 逐步揭示隐藏在文件删除操作背后的隐藏着深层次技术问题甚至政治问题。

一、方案设计

(一) 工具准备

文件恢复过程实质是对存储空间的内容的搜索过程, 当存储容量比较大时, 花费的时间长达数小时。显然, 在课堂上演示如此一个长过程是不可能的, 并且乏味。

可供恢复的存储介质有两类: 硬盘和 U 盘。现在的硬盘容量都高达数百 G, 文件恢复过程甚至长达 4 小时以上; 如果在课堂上演示, 需要拆装硬盘, 与现行的教学设备管理规定相冲突。U 盘是最合适的选择, 但不是什么 U 盘都合适。选择的U 盘应符合两个条件: 2.0 接口, 容量小。

选择好了U 盘以后, 接下来再完成以下工作:

1. 拷贝讲课用的课件文件到 U 盘上, 如 f1.ppt。

2. 在U 盘的根目录下创建一个看上去像被病毒感染的文件。如创建目录 autorun.inf, 很多学生都知道以这种名字命名的目录往往是病毒创建的。

(二) 巧设机关, 欲擒故纵

来到课堂上, 和以往一样首先介绍今天的讲授主题是信息存储安全。然后, 按以下步骤进行。

1. 把准备好的U 盘插入教室的 PC 机 USB 接口。

2. 打开U 盘, 显示出U 盘上的 autorun.inf。此时, 敏感的同学会主动提醒老师 U 盘被病毒感染了。于是, 惊呼: “U 盘被病毒感染了! 赶快删掉!”

3. 迅速按 Ctl-A 组合键, 选择所有的文件, 再按 shift-delete 组合键、回车键, 删除掉所有文件。注意, 这一组动作要迅速、自然, 学生会感觉老师在此方面很专业, 更加信任你。然后, 轻松地吁一口气说, “这下好了, 没问题了!”

4. 稍作停顿。惊呼: “完了! 我把课件给删掉了!” 作焦急状……

5. 赶快查看回收站。“回收站里也没有文件, 这下课上不成了……”。此时, 底下同学一片窃窃私语, 有人甚至高兴今天不用上课了。做沮丧状……

6. 环顾四周, 仔细观察学生的反应。如果所教班级不是大学新生, 或者有同学对计算机很熟悉, 就很可能有同学大声报告: “老师, 有工具可以恢复出被删除的文件!” 如果没有同学大胆提出解决方案, 可以故意问: “我好像听到有人在小声说‘可以用工具恢复’。是这样的吗?”

7. “那太好了! 谁那里有工具啊?”

8. 如果同学举手表示他那有工具, 就表示谢谢。然后, 把笔记本电脑从包里拿出来, 说: “呵呵! 我这笔记本里除了有刚才删除的课件外, 刚好也有这个恢复工具软件。”

9. 同学哗然! 原来老师在欺骗他们, 学生的情绪一下子高昂起来。

(三) 揭示文件删除的原理

有了上述热烈的气氛, 接着向同学们抛出以下问题: 文件明明是删除了, 为什么还被恢复出来了呢? 可以从以下几个方面来揭秘“骗局”的原理。

1、硬盘的存储原理

磁盘的存储原理比较简单。磁盘表面被划分成一个一个的称为“磁道”的同心圆; 盘面被划分为等角度的区域, 称为“扇区”; 磁道落在一个扇区的部分就称为“块”, 通常一个块能够存储 512 字节的数据信息。

从安全保密角度看, 讲解存储原理时特别需要讲透存储单元分配问题。从上述存储原理看, 学生很容易认为磁盘空间分配的最小单元是“块”。这是不对的, 最小的分配单元是“簇”, 即连续的几个“块”。

* [收稿日期] 2009-02-26
[作者简介] 何鸿君 (1968-), 男, 湖南邵阳人, 国防科技大学计算机学院副教授, 博士, 硕士生导师。

由于分配单元是“簇”，很容易造成存储空间闲置问题。只要文件的大小不等于“簇”大小的整数倍，就会造成空间闲置。例如，假设“簇”大小为 8 个块（4KB），一个文件的大小为 2KB。那么，需要为该文件分配一个“簇”，结果有2 个“块”闲置。

讲解至此，可以向同学提问：这些闲置的“块”可以用来干什么呢？同学们都是聪明人，立刻明白可以用来存储其它信息，例如一个文档中的敏感信息。那么，这是谁干的呢？可以是操作系统，也可以是其它高优先级别的程序。

2、删除文件的本质

明白了存储原理，勤于思考的学生还是会觉得奇怪：文件不是删掉了吗？怎么还有恢复出来呢？这时，就可以讲删除操作的本质了。

可以首先问学生是不是有误操作的经历。答案是肯定的。那么，就应该告诉学生，文件删除有时也会有误操作，用户希望有挽救的措施。这种挽救措施当然就是“假”删除，仅仅做一个删除标记，而不是把文件占用的存储块用 0 或 1 清除一遍。其次，从效率角度看，“假”删除比“真”删除需要的时间少得多。

硬盘一般分成主引导扇区、操作系统引导扇区、文件分配表（FAT）、目录区（DIR）和数据区（Data）五部分。在文件删除与恢复中，起重要作用的是“文件分配表”的“目录区”。目录区中的信息定位了文件数据在磁盘中的起始保存位置、文件属性、文件大小等。在定位文件时，操作系统会根据目录区中记录的起始单元，并结合文件分配表区知晓文件在磁盘中的具体位置和大小。

删除文件，其实是修改文件分配表的前 2 个字节，为文件作了删除标记，同时将文件所占簇号在文件分配表中的记录清零，以释放该文件所占空间。这样，文件被删除后硬盘剩余空间增加了，而文件的真实内容仍保存在数据区，如果这些簇的信息不被后来保存的数据覆盖，它就不会从磁盘上抹掉。恢复工具就是利用这个特性来实现对已删除文件的恢复。

恢复文件，其实就是用恢复软件的查找分析功能找出文件头，重写前 2 个字节，并修改文件分配表中的映射记录。仅仅是删除的文件，恢复起来比较容。但是，文件被删除后，如果它所占的簇被存入其他数据，文件头也被覆盖，这个文件在文件分配表中的信息就会被新的文件映射所代替，这个文件一般也就无法恢复了。

3、格式化的本质

讲到这里，较真的学生可能主动提出问题：硬盘都格式化了，为什么还可以恢复出文件、上网记录呢？格式化是什么？

格式化分为高级格式化和低级格式化。高级格式化是对分区表进行清零操作，只是简单地在分区表开头写入一个标识，让系统认为这是一个空的分区而已。实际上原来的数据依然存在。这也是大部分数据恢复软件能够做数据恢复的前提。

低级格式化是将硬盘划分出柱面和磁道，再将磁道划分为若干个扇区，每个扇区又划分出标识部分 ID、间隔区 GAP 和数据区 DATA 等。低级格式化是高级格式化之前的一件工作，每块硬盘在出厂前都进行了低级格式化。低级格式化是一种损耗性操作，对硬盘寿命有一定的负面影响。如果真正对硬盘进行了低级格式化，那么所有存储“块”都被清除了，一般就无法恢复出原来的数据了。

二、开放式训练

问题：如果你来设计硬盘，你可以怎样进行窃密？或者说，你可以怎样对付低级格式化之类的数据清除手段？

在我们的教学实践中，一提出这个问题，学生的思路一下子就打开了。很快就会给出各种各样的解决方案：硬盘中包含有隐藏区域，只能通过不公开的指令进行访问；对硬盘的低级格式化指令进行修改，并不真正清除“块”中的内容；虚报硬盘有大量的损坏磁道，利用这些磁道存储敏感数据文件，等等。

讨论到一定程度，可以很明确地告诉学生，他们的说法都很有道理，很多都是在现有技术条件下可以实现的。事实上，硬盘技术发展迅速，很多方面发生了变化，如用户能访问的是经过转化后的逻辑扇区，而不是实际的与物理磁头对应的物理扇区。这样，用户实际上已经无法对物理意义上的硬盘进行操作了。现在所谓的低级格式化只不过是实现了重新置零和将坏扇区重定向罢了，并不能实现硬盘再生，也没有物理意义上的修复功能。

三、结束语

在两个不同的学期，针对文件存储安全教学主题，分别对多个不同的班级尝试“欲擒故纵”式教学手法，均取得了良好的教学效果。从考试得分情况看，几乎没有学生在硬盘格式化相关的题目上丢分。此外，我们也对教学调查问卷进行了分析统计，学生普遍反映对该堂课的印象非常深刻。

[参考文献]

[1] 林建超，钱海皓. 军事保密学[M]，北京：军事科学出版社，2007.

[2] 赵战生，杜虹，吕述望. 信息安全保密教程[M]，北京：中国科学技术大学出版社，2006.

[3] 罗宇，邹鹏，吴刚. 操作系统[M]，北京：电子工业出版社，2005.

（责任编辑：阳仁宇）