据CNET News.com网站报道，研究人员发现，敲击键盘的声音录音能够转换为键盘输入的内容。这个技术的原理是，由于每一个按键的敲击声音都是与众不同的，即使用户每分钟输入300个字符也会在每次敲击键盘之间留下足够的间隔时间让计算机把每一个声音独立地记录下来。研究人员能够记录用户敲击键盘的若干个10分钟的声音，然后把这些声音输入到计算机，采用一种算法能够恢复96%的输入的内容。   
  
　　这种技术可使用现成的录音设备，在背景有音乐或者手机铃声的时候也能够使用，甚至对“静音”键盘也可以使用。美国加州大学伯克利分校计算机科学与信息管理专业的教授、这项研究工作的主要审查者Doug Tygar表示，虽然这项技术能过盗窃任何打字文件的内容，但是，这项研究重点强调了口令的安全漏洞。   
  
　　他说，口令是一种身份识别的机制。这种方法真的应该重新考虑了。这种攻击并不神秘。这种攻击需要一些计算机知识，不过，使用很多种组件都可以完成这个任务。我们使用了一个价值10美元的麦克风。   
  
　　这项研究工作是在IBM的Dmitri Asonov和Rakesh Agrawal两个人的研究结果的基础之上进行的。他们的研究成果能够从键盘录音中恢复80%的输入的内容。不过，这项试验是在严密的控制之下进行的。   
  
　　这项研究结果将在今年11月10日举行的美国计算机协会会议上公布。加州大学伯克利分校的研究人员研究的这种技术采用了作为搜索引擎的基础的概率计算技术。这种计算机为每一个键盘的按键声音分类，采用有根据的、有知识性的猜测方式推测输入的字符。这种计算机采用键盘声音和语音学的方式来猜测输入的字符。例如，如果在TH后面输入的一个字符声音很相似，计算机会把这个字符猜测为E而不是Q。   
  
　　首次分析字符的准确率为60%，整个单词的正确率为20%。然后，通过计算机进行拼写和语法分析，字符准确率可提高到70%，单词准确率可提高到50%。这个结果然后再输入到计算机对未来的记录结果进行分析。经过三个周期之后，单词的准确率可提高到88%，字符的准确率可提高到96%。  
  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
攻击思路附上：  
如果我打电话给要攻击的目标，尽量的拖延时间跟他聊天，时间长了后他电脑的屏幕保护程序启动了，我估计时间差不多的时候我再诱使他访问一个网站，他回车键入了屏幕保护密码访问了我的网站，而我通过电话听到了键盘记录的声音（可以录下来放大并分离出目标声音）再利用上面文章讲的技术还原他的密码。。。。