网上银行等电子支付平台的 WEB 登陆安全性简要分析

xyzreg 〈http://www.xyzreg.net〉

前言：本文还是去年年初写的，当时出于安全考虑没放出来。现在部分网上银行已大幅度降低了无高级别安全措施情况下的转账限额，并建议用户使用动态口令卡或者 USB Key，总体安全系数有所提高。

随着电子商务的普及，网上银行以及在线电子支付等方式逐渐被网民所接受和喜爱。但是网上银行以及电子商务支付平台的安全性不容乐观。尽管各网上银行采取 SSL 加密防止通过嗅探网络封包的方式截取密码；对于防止 WEB 登陆时密码被窃取，网上银行采取了安全控件或者动态软键盘的方法，**但考虑的仍不全面，我们还是能采取相应的方法截获用户输入的密码。**

下面就以具有代表性的**四大银行：中国工商银行、中国农业银行、中国建设银行、中国银行；商业银行：招商银行；电子支付平台：阿里巴巴支付宝等为例，分别就客户端密码方面进行脆弱性分析。**网上银行以及其他电子商务支付平台的 WEB 登陆安全性直接与用户的经济利益相关，所以有必要不遗余力的加强 WEB 登陆安全性的建设。另外由于不是所有的用户都使用数字证书和 U 盾之类安全认证产品，所以“黑客”只要截取到用户的登陆密码以及支付密码就能随心所欲的转帐/支付，危害甚大。

本文谈的采用纯技术截取密码，而不是用假页面假接口等钓鱼方式骗取密码的方法。

网上银行对于防止密码被盗分别采用了安全控件和动态软键盘的方法：

1、采取安全控件的，典型代表有：中国工商银行、招商银行、阿里巴巴支付宝等

这类安全控件考虑还算全面，防止了键盘/消息钩子，而且使通过 IE 的 COM 接口获取密码的方法也无能为力。但是这类安全控件做得不够底层，考虑得欠深入。

我们采用键盘过滤驱动的方法就可以突破安全控件的保护记录密码了。除了键盘过滤驱动方法外还可以挂接 IDT（中断描述符表）的键盘入口，或者挂钩键

盘驱动 Dispatch 例程以及 Inline hook 相应 IRP 分发函数。 当然，更深入点的话还可以挂钩 i8042prt.sys。

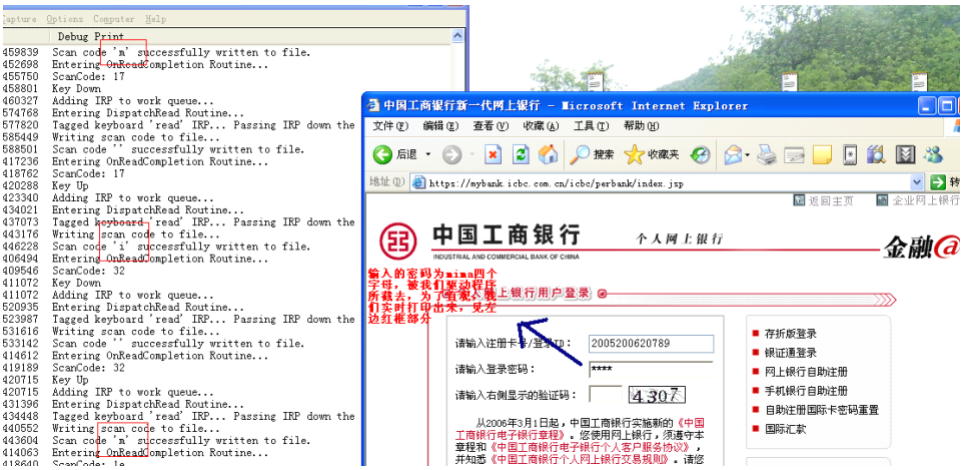
不过由于编写驱动程序不同与开发普通的应用程序，难度稍大，所以目前还未见公开的采用此技术截取这些网上银行密码的木马。但是开发起来也并不是太困难，相对而言采取键盘过滤驱动的方法较通用稳定。

基本原理是我们的驱动创建一个设备附加到键盘驱动 Kbdclass 下的设备，这样所有的 IRP（输入输出请求包）包都将先发给我们的驱动程序，然后再转发给系统中的键盘驱动，我们的驱动程序获取 IRP 后就可以从中获得键盘的 scancode 扫描码，这样就能在**系统内核的层面**获得键盘输入信息。键盘过滤驱动的部分代码如下：

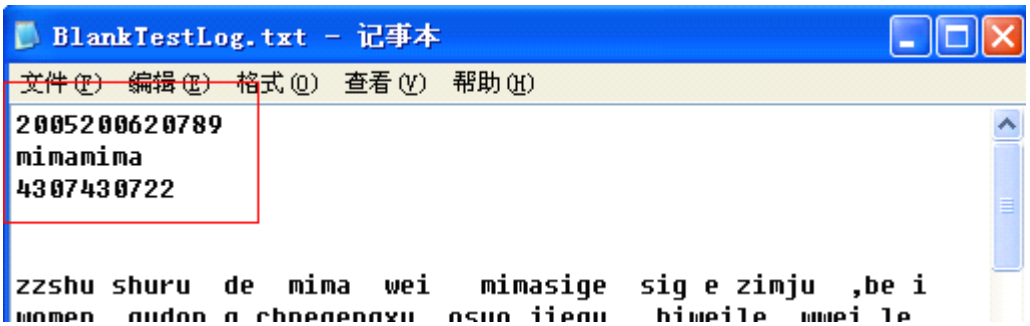
```
NTSTATUS HookKeyboard(IN PDRIVER_OBJECT pDriverObject)
{
 PDEVICE_OBJECT pKeyboardDeviceObject;
 NTSTATUS status = IoCreateDevice(pDriverObject,sizeof(DEVICE_EXTENSION), NULL,
FILE_DEVICE_KEYBOARD, 0, true, &pKeyboardDeviceObject);
 pKeyboardDeviceObject->Flags = pKeyboardDeviceObject->Flags | (DO_BUFFERED_IO |
DO_POWER_PAGABLE);
 pKeyboardDeviceObject->Flags=pKeyboardDeviceObject->Flags&
~DO_DEVICE_INITIALIZING;
 RtlZeroMemory(pKeyboardDeviceObject->DeviceExtension, sizeof(DEVICE_EXTENSION));
 PDEVICE_EXTENSION
pKeyboardDeviceExtension=(PDEVICE_EXTENSION)pKeyboardDeviceObject->DeviceExtension;
 CCHAR ntNameBuffer[64] = "\\Device\\KeyboardClass0";
 STRING ntNameString;
 UNICODE_STRING uKeyboardDeviceName;
 RtlInitAnsiString( &ntNameString, ntNameBuffer );
 RtlAnsiStringToUnicodeString( &uKeyboardDeviceName, &ntNameString, TRUE );
 IoAttachDevice(pKeyboardDeviceObject,&uKeyboardDeviceName,&pKeyboardDeviceExten
sion->pKeyboardDevice);
 RtlFreeUnicodeString(&uKeyboardDeviceName);
 return STATUS_SUCCESS;
}
```

下面以工商银行的网上银行为例，演示我们的程序。为了演示，我们的驱动程序将实时打印出获得的键盘记录的信息，并且把完整的信息记录到磁盘文件上。招商银行、阿里巴巴支付宝等效果等同，支付密码用此法同样能截取。截取

时实时打印的信息 **如图 1**：



记录到文件里的完整信息：**如图 2**：



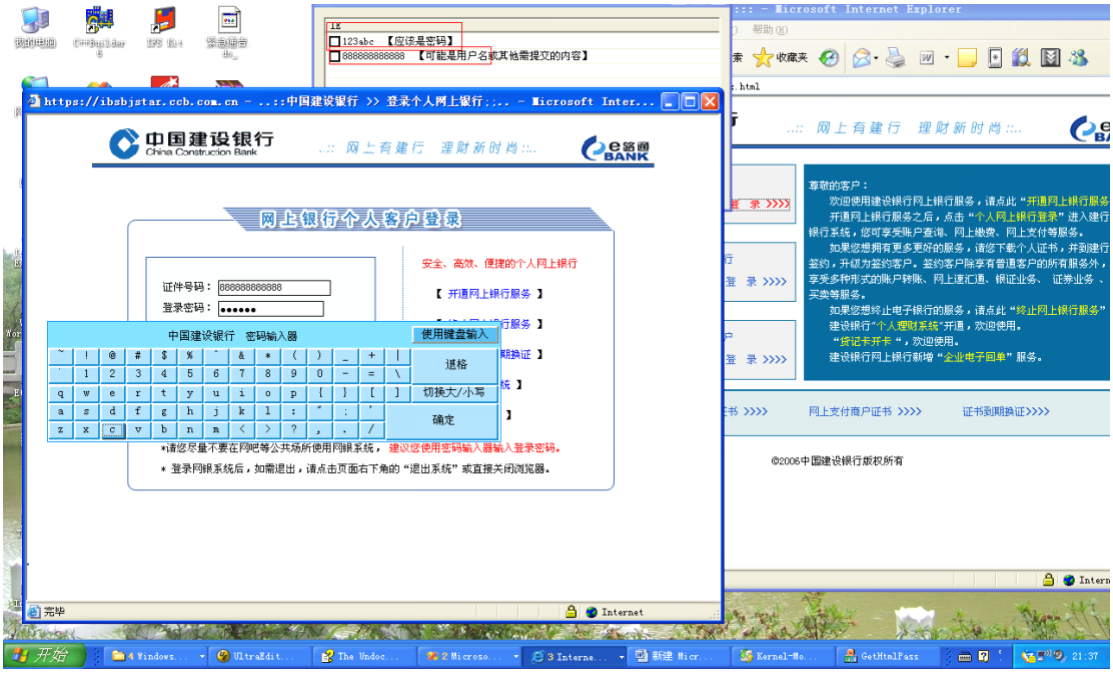
配合发送邮件或者 ASP/PHP 留言的方式我们就能远程的得到密码。

2、采取动态软键盘的，典型代表有：中国建设银行、中国银行、中国农业银行

采用动态软键盘技术初看确实能使攻击者无法截获密码，但是截取密码的方法不仅仅是接截获键盘记录一种方法。我们可以通过 IE 的 COM 获取的密码。

对于中国建设银行，通过 IE 的 COM 接口获取的密码框里的内容就是密码，其他大部分采用软键盘技术的网站大都也是这样。但是中国农业银行 WEB 程序中做了一点处理，通过鼠标点击软键盘传入密框的内容不是实际密码而是按钮序号，所以我们只要枚举当前窗口，发现是中国农业银行的网上银行页面时，我们的程序就自动截图发给我们，我们根据所截获得的图象和通过 IE 的 COM

接口所获得的序号伪密码之间的关系进行转换（抽象为一个简单的函数映射），很容易的。这样便获得了农行网上银行的密码。下面是截取中国建设银行网上银行密码的演示截图，利用动态软键盘的其他网站效果相同。**如图 3**:（衍生：对付应用程序的部分软键盘可以运用 Hook TextOutW/A 的类似屏幕取词的方法来截取。）



后记

尽管网上银行等电子支付平台在密码防盗方面做了安全考虑，但是还是不够安全。不过大家也大可不必因此不使用网上银行，采取数字证书以及 USB Key（比如 U 盾)等安全措施相对而言还是比较安全的。