PHYSICAL SECURITY ATTACKS ON WINDOWS VISTA

Peter Panholzer
SEC Consult Vulnerability Lab, Vienna, 03/05/2008

There are several attacks known today which leverage physical access to fully patched systems to read or patch system memory. One of them is the Cold Boot Attack (1), which allows copying the system memory after the system has been powered off and extracting the keys of encrypted harddisks from it. Another technique known for years now is the copying and manipulation of memory using firewire which, among other things, also can be used to retrieve encryption keys.

Several papers describe the technical background of the firewire attack (2) (3). In a nutshell, it is possible to access the system memory of other nodes on a firewire bus via DMA and firewire's addressing scheme. This works for reading as well as for writing. The only requirement on the target is a firewire interface, which most laptops and a lot of workstations have built in. Laptops without a firewire interface can be provided by an attacker with a PC Card (PCMCIA Card) which is automatically installed – even if the screen is locked. This means that even laptop computers without a firewire interface are vulnerable. It has been proven that Linux, MAC OS X and Windows XP are vulnerable to this attack. In March 2008, Adam Boileau released a tool called winlockpwn (4), which implements several attacks against Windows XP SP2.

A while ago, SEC Consult has implemented its own proof of concepts for most versions of Windows. This includes workstations running Windows Vista. The Vista POC disables password authentication in the default login routine, making it possible to log in to the workstation with an arbitrary password. What follows is a high level overview of our Vista unlock tool[1].

In Windows Vista, NTLM authentication is performed by the NTLM security support provider, Msv1_0.dll, which is used to authenticate against the SAM database. During our tests, its code segment was always found in physical memory, making it possible to perform a patch at any time.

Adapting the unlock hack to Vista basically boils down to finding the correct code location for applying the patch. In Vista, the actual password comparison is done with a call to `RtlCompareMemory()` in the function `MsvpPasswordValidate()` of MSV1_0.dll (figure 1). By patching the subsequent conditional jump with NOP-Instructions, the memory comparison is effectively disabled.

[1] Due to SEC Consult´s disclosure policy, we are not allowed to release the tool itself.

```
.text:6DDCB429 loc_6DDCB429:                           ; CODE XREF: MsvpPasswordValidate(x,x,x,x,x,x,x)+8E↑j
.text:6DDCB429                                         ; ReferenceSubAuth(x,x)+7F7↓j
.text:6DDCB429                 push    10h             ; Length
.text:6DDCB42B                 add     ebx, 34h
.text:6DDCB42E                 push    ebx             ; Source2
.text:6DDCB42F                 push    esi             ; Source1
.text:6DDCB430                 call    ds:__imp__RtlCompareMemory@12 ; RtlCompareMemory(x,x,x)
.text:6DDCB436                 cmp     eax, 10h
.text:6DDCB439                 jnz     short loc_6DDCB44E
```

FIGURE 1: PASSWORD VERIFICATION

In short, our Vista unlock tool uses signature matching to find the respective binary code in the target node´s memory (the same method is used in winlockpwn). The process of searching the pattern and manipulating the DLL code in memory takes a few seconds up to a few minutes. After the patch has been applied, any username and password can be specified at the login prompt for a successful login.

The manipulation of the authentication process is just one of many possibilities. Insertion of Malware or opening a shell would be others. It is also possible to do a full memory dump and search for harddisk encryption keys, just like the Cold Boot Attack, but without having to reboot the system. These attacks too work on Windows Vista targets.

There is no security update provided by Microsoft and possibly never will be as these attacks are not based on a vulnerability but merely are possible because of the designs and protocols. The only known effective way of protecting against the firewire attack is to deactivate all firewire and PC Card ports in the device manager. The device manager of Windows Vista can be accessed via Start → Control Panel → System and Maintenance → System → Device Manager. Right click on all firewire and PC Card (PCMCIA) ports and choose deactivate. There is no known countermeasure against the cold boot attack at the moment but restricting physical access to your systems.

About the Vulnerability Lab

Members of the SEC Consult Vulnerability Lab perform security research in various topics of technical information security. Projects include vulnerability research and the development of cutting edge security tools and methodologies, and are supported by partners like the Technical University of Vienna. The lab has published security vulnerabilities in many high-profile software products, and selected work has been presented at top security conferences like Blackhat and DeepSec.

For more information, see http://www.sec-consult.com/.

REFERENCES

1. **Halderman, Alex J., et al.** Lest We Remember: Cold Boot Attacks on Encryption Keys. [Online] February 21, 2008. [Cited: February 29, 2008.] http://citp.princeton.edu.nyud.net/pub/coldboot.pdf.

2. **Boileau, Adam.** Hit by a Bus: Physical Access Attacks with Firewire. [Online] 2006. [Cited: February 29, 2008.] http://storm.net.nz/static/files/ab_firewire_rux2k6-final.pdf.

3. **Becher, Michael, Dornseif, Maximillian and Klein, Christian N.** FireWire: all your memory are belong to us. [Online] 2005. [Cited: February 29, 2008.] http://md.hudora.de/presentations/firewire/2005-firewire-cansecwest.pdf.

4. **Winlockpwn (tool)** http://storm.net.nz/static/files/winlockpwn