Subject: Re: sec : U Re: travelling idl license
Posted by Randall Skelton on Wed, 25 Sep 2002 17:31:12 GMT
View Forum Message <> Reply to Message

On Wed, 25 Sep 2002, Andrew Cool wrote:

> Hi Randall,
>
> On Windows at least, the MS Information tool will return the serial
> number of the Hard Drive.

Hi Andrew,

Unfortunately, these 'serial numbers' are not at all related to the physical disk but rather, are an IBM/Microsoft concoction designed originally to allow the windows to keep track of which disk is which. Basically, in 1987 when Microsoft and IBM were co-developing OS/2, they wanted to write a system that would automatically recognize a disk (hard disk, floppy, optical, etc) like a Macintosh could do in system 6. Thus, a 4-byte, 'volume serial number' (VSN) residing in the boot sector was added to the standard DOS format. When a disk is formatted in windows it is stamped with this four-byte number which is constructed from the exact date and time the format operation was performed. Utilities like disk copy will copy everything except this four-byte string. However, there are many other utilities that can change this field to match any desired time stamp so it is hardly a viable method of copy protection-- this, of course, doesn't prevent some companies from using it.

So there are really 2 noteworthy points. Firstly, the VSN was never indended to be used as a firm method of authentication. While the byte code format and location in the boot sector has changed for FAT16, FAT32, NTFS, etc, the specifications are wide open and the number is easy to spoof (see <http://www.sysinternals.com/ntw2k/source/misc.shtml> and look for the utility named 'volumeid'). Second, it is impossible to have IDL for *nix and Windows on the same physical disk with the license tied to the VSN because provision for including it are not made by other file systems (ext2, xfs, ufs, hfs, hfs+, etc). There are no provisions in the IDE or SCSI interface specifications to provide a unique hardware id.

At this point, the only way to physically license software is with a dongle (i.e. HASP) or an ethernet card.

Cheers,
Randall

Subject: Re: sec : U Re: travelling idl license

"Randall Skelton" <rhskelto@atm.ox.ac.uk> wrote >

> There are no provisions in the IDE or SCSI interface
> specifications to provide a unique hardware id.

I don't think this is true. From a casual browsing of google.groups I read a number of posts which state that there has been a spec for HDD serial numbers since ATA-1. This has been carried on into ATA-2 and ATA-3. Although there is nothing requiring manufacturers to implement this I beleive that many today do. I spent less time looking for SCSI references on this topic but I believe that SCSI devices have implmented something similar as well.

And I am not talking about the 4 byte VSN.

My search terms were: "'hard drive serial number' +ATA"

> So there are really 2 noteworthy points. Firstly, the VSN was never
> indended to be used as a firm method of authentication.

> Second, it is impossible to have IDL for *nix and Windows on the
> same physical disk with the license tied to the VSN because
> provision for including it are not made by other file systems
> (ext2, xfs, ufs, hfs, hfs+, etc).

Your points are valid, assuming that the FlexLM system uses the 4 byte VSN. From what I can tell it *does* which makes it pretty much useless. So yes, I agree that HASP and MAC addresses are probably the most robust. And all of this is academic since RSI is only using the MAC address when generating licenses anyway.

RSI could issue dongles using FlexLM instead of HASP. I am assuming that they dropped HASP after counting some beans. Since they will still be maintaining the FlexLM code in IDL and paying the license fees one would assume that offering hardware keys using FlexLM would come at a significant savings over HASP allowing them to still offer "portable" secure licenses available for all of their supported platforms (not just the popular ones). But I am mostly talking out my rear on this.

Bob: You could be the guinea pig for us HASP users. It would be worth trying to license IDL to a PCMCIA NIC and use that as your dongle. You of course would have to get a PCMCIA card reader for your desktop. It should work, the only issue would be managing the multiple NIC's in the machine. I

don't know how the license manager selects the NIC on a machine with multiple network interfaces though. It looks like it takes the first one it finds which would complicate this a bit. You want to try that out and get back to us? ;)

Also, How does this personal license work. Say I have a work machine, laptop, and home machine (all running the same OS). Currently I can carry my dongle in my pocket and work wherever I want. How does the personal license "float"?

-Rick

Subject: sec : U Re: travelling idl license
Posted by Andrew Cool on Thu, 26 Sep 2002 03:04:26 GMT
View Forum Message <> Reply to Message

Randall Skelton wrote:
>
> On Wed, 25 Sep 2002, Andrew Cool wrote:
>
>> Hi Randall,
>>
>> On Windows at least, the MS Information tool will return the serial
>> number of the Hard Drive.
>
> Hi Andrew,
>
> Unfortunately, these 'serial numbers' are not at all related to the
> physical disk but rather, are an IBM/Microsoft concoction designed
> originally to allow the windows to keep track of which disk is which.
> Basically, in 1987 when Microsoft and IBM were co-developing OS/2, they
> wanted to write a system that would automatically recognize a disk (hard
> disk, floppy, optical, etc) like a Macintosh could do in system 6. Thus,
> a 4-byte, 'volume serial number' (VSN) residing in the boot sector was
> added to the standard DOS format. When a disk is formatted in windows it
> is stamped with this four-byte number which is constructed from the exact
> date and time the format operation was performed. Utilities like disk
> copy will copy everything except this four-byte string. However, there
> are many other utilities that can change this field to match any desired
> time stamp so it is hardly a viable method of copy protection-- this, of
> course, doesn't prevent some companies from using it.
>
> So there are really 2 noteworthy points. Firstly, the VSN was never
> indended to be used as a firm method of authentication. While the byte
> code format and location in the boot sector has changed for FAT16, FAT32,

> NTFS, etc, the specifications are wide open and the number is easy to
> spoof (see <http://www.sysinternals.com/ntw2k/source/misc.shtml> and look
> for the utility named 'volumeid'). Second, it is impossible to have IDL
> for *nix and Windows on the same physical disk with the license tied to
> the VSN because provision for including it are not made by other file
> systems (ext2, xfs, ufs, hfs, hfs+, etc). There are no provisions in the
> IDE or SCSI interface specifications to provide a unique hardware id.
>
> At this point, the only way to physically license software is with a
> dongle (i.e. HASP) or an ethernet card.
>
> Cheers,
> Randall

Hiya Randall,

You lost me about line 3, I think. But below is what I know can be done. Three doors down the corridor from me is a guy running this licence on a dual boot Windows/Linux laptop.

Keyed to the DSN, no less.

I've changed the encryption sequences least anybody gets any funny ideas ;-)

Regards,

Andrew

```
INCREMENT idl_drawx idl_lmgrd 1.000 1-jan-0000 0 FB06C092384AD3DD4DD3 \
  VENDOR_STRING="4434Surv Systems Div, DSTOS" \
  HOSTID=HOSTNAME=lightstar ck=2
INCREMENT idl_drawx idl_lmgrd 1.000 1-jan-0000 0 4BB651F188C648B20C26 \
  VENDOR_STRING="4434-1Surv Systems Div, DSTOS" \
  HOSTID=DISK_SERIAL_NUM=d82b5aef ck=191
INCREMENT insight idl_lmgrd 2.000 1-jan-0000 0 8B1390B18418A5C7B8CC \
  VENDOR_STRING="4434Surv Systems Div, DSTOS" \
  HOSTID=HOSTNAME=lightstar ck=13
INCREMENT insight idl_lmgrd 2.000 1-jan-0000 0 8B567002F73BD110364D \
  VENDOR_STRING="4434-1Surv Systems Div, DSTOS" \
  HOSTID=DISK_SERIAL_NUM=d82b5aef ck=217
INCREMENT idl idl_lmgrd 5.400 1-jan-0000 0 CDF662815FF028A145E8 \
  VENDOR_STRING="4434Surv Systems Div, DSTOS" \
  HOSTID=HOSTNAME=lightstar ck=37
INCREMENT idl idl_lmgrd 5.400 1-jan-0000 0 8BB6F0C1549A12E40A95 \
  VENDOR_STRING="4434-1Surv Systems Div, DSTOS" \
  HOSTID=DISK_SERIAL_NUM=d82b5aef ck=15
```

#
--

-- ----------------
Andrew D. Cool .->-.
Electromagnetics & Propagation Group '-<-'
Intelligence, Surveillance & Reconnaissance Division Transmitted on
Defence Science & Technology Organisation 100% recycled
PO Box 1500, Edinburgh electrons
South Australia 5111

Phone : 061 8 8259 5740 Fax : 061 8 8259 6673
Email : andrew.cool@no-spam.dsto.defence.gov.au
Please remove the no-spam from my email address to reply ;-)
-- ----------------