

Re: Can a program prove it's own integrity?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-05/5059.html>

From: AE (*hidden_at_nospam.com*)

Date: 05/20/04

Date: Thu, 20 May 2004 10:09:12 +0200

sounds good to me :-)

It's a slow and fairly complex procedure, but since it's done only in case the boot floppy is broken and has to be replaced it can be done.

Kiuhnm wrote:

> AE wrote:

>

>>This is where the idea comes from:

>>

>>I wanted to protect a complete harddisk – encrypting disk driver,
>>modified bootloader to run the operating system from the encrypted
>>disk.

>>

>>The weak point is the bootloader: If it is changed an attacker can
>>read the password as I'm typing it and all security is gone.

>

>

> Write a self-decrypting pre-bootloader that, in order to work properly and
> eventually decrypt the real bootloader on the hard disk, needs some random
> data.

> Put the pre-bootloader and the random (or compressed cryptographic) data on
> a floppy disk. Your floppy disk must be **full** and the data nearly

> incompressible (just use a state-of-the-art compressor).

> The encrypted part of the pre-bootloader, once decrypted and executed, must
> enter the highest privilege level (e.g. Ring 0), use time-stamp instructions
> and execute **many** difficult-to-emulate operation (the code could test the
> "protected mode" functionalities..., execute pmode BIOS extension, etc...).

> The code will also check the floppy disk hash and print "expected secret
> strings" on the screen.

>

> You could use a low-density floppy disk (it's more efficient because you
> have less data).

>

> You should:

> 1) (physically) disconnect the hard disk,

> 2) (physically) write-protect the floppy and insert it,

sci.crypt: Re: Can a program prove it's own integrity?

- > 3) *turn on your computer,*
- > 4) *insert the password,*
- > 5) *wait :-)*
- > 6) *Examine the screen and decide if the floppy disk is genuine.*
- > *If you think it's genuine:*
- > 7) *turn off your computer,*
- > 8) *reconnect the hard disk,*
- > 9) *turn on your computer,*
- > 10) *etc...*
- >
- > *Notes:*
- > – *your hard disk must be disconnected or the attacker could copy partial*
- > *data of the floppy to the hard disk (even if it's encrypted);*
- > – *your pre-bootloader should even check hashes of your BIOS, etc...*
- > – *Once your software enters Ring 0, no one can completely control it. One*
- > *can only run that program in a virtual machine and still it's very difficult*
- > *to emulate perfectly all the functionalities and handle accurately all the*
- > *time-stamp instructions. Anyhow, a virtual machine requires a lot of code*
- > *and it's practically impossible to compress the data in the floppy in order*
- > *to create enough space for the virtual machine.*
- > – *When you find out that the floppy is compromised, your password could have*
- > *just been saved somewhere in the BIOS, etc...*
- > *This is not a problem: just create another disk and use another password.*
- > *Your true bootloader can't be revealed while you execute the pre-bootloader*
- > *with the hard disk disconnected.*
- >
- > *Kiuhnm*
- >
- >