Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Why Bother About BIOS Security?

Security is always only as strong as its weakest link. While there do exist many guidelines to secure various operating systems, there is considerably less material available on how to secure the low-level components of a PC, although these can equally be compromised in order to obtain full control over a machine. First this paper gives an overview of the BIOS and its functions. Then known threats to the BIOS and the hardware of a PC are discussed in detail and how they could be exploited. Finally countermeasures are g...

Copyright SANS Institute
Author Retains Full Rights

AD

Why bother about BIOS security?

Robert Allgeuer
July 23, 2001

Abstract

Security is always only as strong as its weakest link. While there do exist many guidelines to secure various operating systems, there is considerably less material available on how to secure the low-level components of a PC, although these can equally be compromised in order to obtain full control over a machine.

First this paper gives an overview of the BIOS and its functions. Then known threats to the BIOS and the hardware of a PC are discussed in detail and how they could be exploited. Finally countermeasures are given that can mitigate the risks.

BIOS Overview

The motherboard inside every PC would not do anything if there were not a special program that takes control after the PC is switched on. This program is called the BIOS (Basic Input/Output System).

Important tasks of the BIOS are to perform a power up test of hardware components and memory, to initialise hardware and finally to search for an operating system that can be booted. For doing so it loads the first sector of the diskette or hard disk into memory, performs a short validity check and executes the code contained in this block. Depending on the type of operating system there may be further steps involved, but essentially this code loads the operating system and passes control to it.

The BIOS also implements input and output routines that used to be called by real-mode operating systems, such as DOS. In modern protected mode operating systems, however, dedicated drivers implement I/O functions, which leaves the BIOS idle once the operating system has been loaded. A more detailed description of the BIOS and the boot process can be found in [1].

On modern motherboards the BIOS program is stored in a chip called a FLASH EEPROM. This chip does not lose its contents, when power is switched off. A FLASH EEPROM can be re-programmed with dedicated flash utilities, which is how the BIOS can be updated to a newer version.

The BIOS also has to maintain state. Any persistent data needed by the BIOS is kept in the so-called CMOS RAM. This chip holds information such as

- Where to check for operating systems to boot (diskette, hard disk, CDROM) and in which order these sources should be tried
- Information about attached hard disks

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Performance parameters such as memory access timing
- Interrupt assignments
- And other information required for the computer to operate

A battery - usually soldered to the motherboard - buffers power for the CMOS RAM even when the computer is switched off, so that its data is not lost. The contents of the CMOS RAM can be configured by means of the BIOS configuration utility that is accessible during boot time upon pressing a special key or key combination. Typical keys are for example DEL, ESC or a function key.

On practically all systems access to the BIOS configuration utility can be controlled by a password, the so-called BIOS password. Once this password is set, the configuration of the computer cannot be changed without knowledge of this password (or at least this is the idea). On almost all systems the BIOS password information is stored in the CMOS RAM.

Finally, not every computer manufacturer produces his proper BIOS. Usually they buy the BIOS from specialised companies such as AMI, AWARD or PHOENIX. The consequence is that there are not so many different BIOS types out there as one might believe.

The Threats

As explained above the BIOS controls, which operating system is started. For that purposes it maintains a parameter, usually called the boot order, which determines, whether the operating system will be loaded from diskette, hard disk, CDROM or in some cases also from the network.

If an attacker succeeds to change this parameter in such a way that software provided by him is executed, rather than the installed operating system, there is no more other way to protect the system from being compromised. The carefully designed secure standard build with its restricted permissions or registry keys or a refined password policy will not help in such a case.

Typically an attacker would boot the system from a diskette that contains software to either change the system's administrator or root password, to extract password information for an offline password attack or to directly access data on the hard disk. The attacker might also install backdoors or Trojans in order to be able to access the system again later or to further extend access to other systems.

This is feasible for any machine, including servers and workstations. Please note, however, that for this attack physical access to the computer is required. Assuming adequate physical protection of servers, this means that workstations are particularly exposed. How many organisations do have a policy to lock all doors during absence? How tight is physical building security in reality? What about insiders?

One might think that protection of workstations is not too important. Maybe one compromised workstation does not matter too much. Wrong! One single workstation

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

can be used as launch pad for further attacks and it is normally easy for the attacker to extend access:

- Key logging programs will record passwords to the domain, servers and applications used on the compromised workstation.
- Sniffing may be used to extract password information that is passing by on the same network segment.

The importance of securing all workstations is discussed in more detail in [2].

So how can BIOS access control be by-passed? We assume of course that a password has been set in the first place and the boot order is correctly set! Basically we distinguish between four different methods [5]:

1. Use of backdoor passwords
2. Cracking the BIOS password
3. Deleting the contents of the CMOS RAM by software
4. Deleting the contents of the CMOS RAM by hardware

In the following we will discuss each of these possibilities in more detail

Backdoor Passwords

It may be hard to believe, but many BIOS manufacturers build in backdoor passwords in their products. Even worse, many of these passwords are easy to guess, such as the name of the BIOS manufacturer. Extensive lists of known backdoor passwords are available on the Internet e.g. [4], [5] and [7] and inside of the software !BIOS [9].

The following non-comprehensive list gives an impression of the 'quality' of those passwords:

Award-BIOS:

```
589589, 589721, Award, AWARD, AWARD SW, AWARD?SW, AWARD_PS,
AWARD_PW, AWARD_SW, j256, j262, J256, J262, J64, q_l27&z, ALFAROME,
BIOSTAR, BIOSSTAR, award.sw, award sw
```

AMI-BIOS:

```
Ami, AMI, AMI_SW, AMI?SW, AMI SW, AMI?PW, A.M.I., oder , Oder,
PASSWORD, amipswd, AMIPSWD, AMIAMI
```

Phoenix-BIOS:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
BIOS, CMOS, phoenix, PHOENIX
```

Others:

```
aLLy, awkward, BIOSTAR, CONDO, HLT
lkwpeter, lkw peter, LKWPETER, SER, setup, SKY_FOX, Sxyz, Syxz,
SZYX, Wodj, merlin, Compaq, central, iwill, bell9, Toshiba, admin,
BIOS, Dell, Posterie
```

Normally BIOS manufacturers are using the American keyboard layout. This has to be taken into account when entering BIOS passwords on international keyboards. For example on a German or Italian keyboard AMI?SW has to be typed in order to be accepted by the BIOS as AMI_SW. BIOS passwords normally are case sensitive.

It seems, however, that on modern systems these known backdoor passwords work less and less often. Tests carried out on PCs with Award BIOSes from 1997 or later had the result that none of the well-known passwords worked, which is good news.

Cracking BIOS Passwords

Almost all BIOSes store their password information in the CMOS RAM. The days of BIOS password storage in clear text seem to be over, modern BIOSes store their passwords in hashes. Unfortunately these hashes are of low quality and short. Award for example calculates only a 16 bit hash, which means that there are numerous collisions and many different passwords will produce identical hash values [6].

This makes password cracking a relatively easy task. Cracking programs do exist for all major BIOS manufacturers [5]. The probably most powerful programs are CmosPwd [8] and !BIOS [9], which support several platforms and algorithms.

Tests with both programs show that successfully cracking BIOS passwords is a matter of seconds or minutes at most. !BIOS also offers a brute force option. During a test this function offered more than thousand valid passwords for an Award BIOS that all produced the given password hash in the CMOS RAM. With this program it is also possible to restrict brute forcing to numbers only, which results passwords that will work independently from the keyboard layout.

It has to be noted that a password cracking attack requires that the attacker has already gained access to the machine before, in order to be able to run the cracking program, which then will read the contents of the CMOS RAM. A mitigating factor, but this is where the problem of commonality [2] comes into play: It is very difficult to manage a good company-wide password policy for BIOS passwords. Therefore chances are that many machines will share the same BIOS passwords and that this password is never changed on a given PC. It will take only one single workstation to which the attacker manages to gain temporary access by any method, in order to break defence for a large number of stations.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Erasing the CMOS RAM by Software

If the methods explained above do not work, an attacker will probably try to erase the contents of the CMOS RAM. On most systems this step will delete all BIOS settings including the BIOS passwords and will reset the values to a factory preset. All that needs to be done then is to enter the BIOS configuration utility after a reboot and to set the boot order to boot from a diskette with tools for changing or removing the operating system's password.

Erasing the CMOS can be achieved by a few simple commands in the DOS tool DEBUG [3]:

```
debug
o 70, 2E
o 71, 0
q
```

There do exist also slightly different variants of these commands, as found e.g. in [4], but the principle always remains the same: these commands write to the I/O ports 70 and 71, which is how to access the contents of the CMOS RAM, in order to invalidate its checksum. This causes the computer to reset the CMOS RAM to default values with no password set at the next reboot.

For those who do not want to deal with DEBUG, dedicated tools for that purpose are also freely available on the Internet, e.g. [5], [8] and [9]. Again, also for deleting the contents of the CMOS RAM by software, an attacker must have gained or been granted access to the computer before.

Erasing the CMOS RAM by Hardware

If an attacker does not have the possibility to run a program on the target machine, he has another option: accessing the computer's motherboard by opening its case and to erase the CMOS RAM by hardware.

Most motherboards do have a jumper for exactly that purpose, which is usually located close to the clock chip and bears a name such as CLRTC, Clear CMOS or PWRD. Normally the procedure to follow is described in the motherboard's manual. Depending on the hardware this may involve to short-circuit the jumper for a few seconds, or to set a jumper and to briefly switch on the computer.

If a motherboard does not offer such a jumper, an option is to remove the buffer-battery for the CMOS RAM chip, which may require unsoldering it. The battery must be kept disconnected for an hour or longer in order to erase the contents of the chip including the password settings.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Finally there is the method of short-circuiting specific pins on the clock chip itself. This is of course dependent on the chip used on the motherboard. Instructions for various commonly used chips are e.g. described in [4] and [3].

Other possibilities

For some specific computers further methods do exist:

- Some Toshiba notebooks reset the BIOS password when a special key-diskette is in the floppy drive during start-up [4].
- Some Toshiba notebooks remove the BIOS password when a special loopback device is connected to the parallel port during start-up [8].
- If the PC has at least one ISA slot, an extension card with an EPROM containing a CMOS erasing routine can be inserted. This routine would then be executed as BIOS extension at the next reboot and erase the CMOS RAM [3].
- If the computer does not enforce a reboot after a certain number of failed authentication attempts, BIOS passwords could also be brute-forced by a second computer connected to the keyboard port simulating a keyboard entering passwords [3]. The collision of hashes for different passwords due to the short hash values used will make this faster than it needs to be.
- Some (probably old) BIOSes skip the password check if either a specific key is pressed during boot (candidates could be Left-Shift, Ins, Del, F1) or both mouse buttons are held down at the same time during boot [9].

Finally, why should an attacker bother to crack the BIOS, if he can gain physical access to the interior of a computer? In this case he might just remove the hard disk altogether, connect it as secondary disk to his home computer (with the BIOS set to auto-detect) and access all data on the disk including password hashes.

Countermeasures

Now that we understand what attackers could do, let us discuss what the countermeasures are that could also be applied in a corporate environment:

- BIOS passwords shall be used on every computer in an organisation in order to protect access to the BIOS configuration utility. In a corporate environment it may be unrealistic to have different BIOS passwords for every computer and to regularly change these passwords on all systems, but as a minimum the BIOS passwords assigned to new machines during installation shall be changed regularly. A possible scheme could be to change the password assigned to newly installed machines every quarter. If the inventory records the installation time of every computer and a history of BIOS passwords is kept in a secured list, it will always be possible to determine the correct password for a given computer.
- BIOS passwords used for critical systems shall be different from those used on less critical and less protected systems.
- All computers shall be set to only boot from their hard drives.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Well-known backdoor passwords and methods shall be tested on every new model that is introduced to an organisation. Computers that are affected shall be avoided.
- All computer cases shall be locked. Mostly computers provide a mechanical lock for that purpose, on some more recent models this can be set as BIOS option.
- Computers shall be physically protected as far as is possible due to their purpose. Machine rooms must have strict access control and all computer shelves shall be locked. For workstation security a policy that offices must be locked during absence shall be considered.
- The policy of the organisation shall state that critical data must not be kept on local hard disks, but exclusively on server storage. Data on laptops shall be encrypted.

Of course this still cannot guarantee perfect security, but if implemented, these measures will reduce the probability of a compromise through the BIOS considerably.

Conclusion

BIOS security must be taken seriously. As a principle security is always only as strong as the weakest link. If the BIOS is not secured properly, it is not only this single machine and the data it holds that is at risk, but actually the complete network. Countermeasures can largely mitigate the risk, although total elimination is impossible.

References:

[1] BIOS Central: BIOS Basics; http://www.bioscentral.com/misc/biosbasics.htm

[2] Marvin, Daniel: The Commonality of Authenticators Vulnerability Relative to NT Local Administrator Accounts; http://www.sans.org/infosecFAQ/win/commonality.htm

[3] Stiller, Andreas: Come right in! - Can BIOS passwords serve as safety bolts?; http://www.heise.de/ct/english/98/08/194/

[4] Qrin, Elf: How to bypass BIOS passwords; http://www.elfqrin.com/docs/biospw.html

[5] Sudden Death: BIOS Passwort knacken; http://www.brandtcomputer.de/SuddenDeath/BIOS.html

[6] Bluefish: BIOS; http://www.safenetworks.com/mUNIXes/bios5.html

[7] Karalius, Mindaugas: BIOS Crack; http://elinara.ktu.lt/~jkmwww/ps04v/mindaugas.karalius/BIOS.htm

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[8] Christophe Grenier: CmosPwd;
http://www.esiea.fr/public_html/Christophe.GRENIER/

[9] Eleventh Alliance; !BIOS; http://www.11a.nu/ibios.htm

© SANS Institute 2002, Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**