

Keamanan BIOS dan Boot Loader

Anda tentu tidak ingin komputer Anda di-*boot* orang yang dikhawatirkan akan mengakses data rahasia atau merusak sistem Linux. Anda dapat mencegahnya dengan memberikan *password* pada BIOS dan *boot loader* GRUB atau Lilo.

Jika dilihat dari sejarah adanya Linux, maka dapat disimpulkan bahwa Linux merupakan turunan dari Unix. Unix mempunyai tingkat keamanan yang tinggi dibandingkan dengan berbagai macam jenis sistem operasi yang ada. Tentunya tingkat keamanan ini juga “diwariskan” kepada Linux. Pada dasarnya, Linux mempunyai tingkat keamanan yang tidak jauh beda dari Unix. Namun, semua itu masih membutuhkan beberapa langkah optimasi lagi agar Linux semakin aman. Tulisan singkat ini berupa petunjuk mengamankan BIOS dan *boot loader*.

Password BIOS

BIOS (*Basic InputOutput System*) merupakan sebuah program kecil yang digunakan untuk mendeteksi dan mengonfigurasi *hardware*. Namun, siapa sangka jika Anda melalaikan seberapa pentingnya BIOS maka bisa saja data Anda akan hilang. Memproteksi BIOS, berguna untuk mengamankan dari user yang tidak berhak mengakses secara fisik kepada system dengan *me-reboot* PC. Sewaktu PC di-reboot, jika BIOS tidak diproteksi maka seseorang dapat memasukkan disket atau CDROM yang digunakan untuk meng-*hack* atau meng-*copy* program jahat ke dalam system. Dengan

booting melalui cdrom atau floppy maka system kita tidak akan aman karena seseorang dapat menjalankan berbagai macam aplikasi ‘hitam’.

Secara umum alasan mengamankan BIOS, yaitu:

1. Mencegah diubahnya konfigurasi pada BIOS.

Jika seseorang dapat masuk ke dalam BIOS, maka dia dapat dengan mudah mengacak-acak system. Men-*disable hardware* atau mengubah urutan booting tentunya akan sangat merugikan bagi komputer yang dijadikan server ketika ditinggalkan oleh administrator. Dengan boot melalui floppy drive atau cdrom seorang penyusup dapat saja dengan mudah menggunakan mode booting dengan mode *rescue* atau *single user mode*. Siapa pun yang paham hal ini tidak akan membiarkan BIOS dengan mudah diakses.

2. Mencegah sistem di-booting oleh yang tidak berhak.

Beberapa jenis BIOS mempunyai fasilitas untuk memberikan *password full* (dua password) terhadap sistem. Maksudnya, sebelum boot loader tampil maka akan muncul prompt untuk memasukkan password. Sehingga di dalam BIOS terdapat dua password, yaitu password ketika akan masuk BIOS dan password ketika akan booting.

Hal di atas jika tidak kita perhatikan dapat saja dengan mudah komputer diacak-acak. Tentunya dengan memaksimalkan keamanan inilah, maka akan menjadikan komputer yang kita gunakan lebih aman. Apabila anda lupa password BIOS maka terdapat dua jalan yaitu:

- *Reset jumper*. Hal ini dapat Anda lihat di buku manual motherboard.
- Melepas CMOS baterai, kemudian memasangnya kembali.

Password boot loader

Boot loader digunakan untuk me-*load* konfigurasi program untuk dijalankan sewaktu booting. Tentunya dengan berbeda jenis sistem operasi maka akan berbeda pula jenis pengamanannya. Kali ini penulis dengan menggunakan RedHat9.0 akan mengonfigurasi password untuk mengamankan boot loader.

Berikut ini alasan utama kenapa harus mengamankan boot loader:

1. Melarang user masuk dengan modus single user.

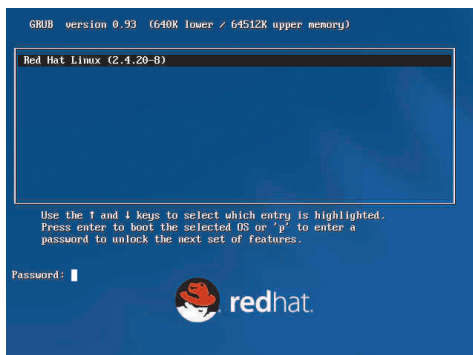
Single user di sini maksudnya seorang yang login kali pertama, maka otomatis menjadi root. Dengan mengetikkan `linux -s` pada prompt boot loader, maka user tersebut otomatis sebagai root. Secara default semua distro Linux membolehkan penggunaan single user mode (`linux single`). Jika hal ini tidak diatasi, maka orang dengan mudah mengacak-acak sistem. Karena hak akses root tak terbatas.

2. Melarang user masuk ke console dari GRUB.

Linux Red Hat atau Fedora menggunakan GRUB sebagai boot loader, mengingat boot loader ini mempunyai keunggulan tersendiri dibandingkan Lilo, misalnya dapat diedit saat boot.

3. Melarang user masuk ke opsi booting yang lain.

Apabila pada komputer tersebut menggunakan dual boot maka bisa saja orang jahil akan masuk ke sistem operasi lain (misal Windows), sehingga dapat dengan mudah mengacak-acak komputer (tentunya dengan bantuan program yang lain). Hal sederhana seperti di atas akan membawa dampak yang berbahaya jika sejak dari dini kita tidak mewaspaidanya.



Gambar 1. Password pada GRUB.

Password pada GRUB

Untuk memberi password pada GRUB dengan memanfaatkan enkripsi, lakukan perintah berikut ini:

1. Ketikkan pada shell (login sebagai root):

```
# /sbin/grub-md5-crypt
```

2. Setelah mengetik perintah di atas, maka akan tampil perintah untuk memasukkan password. Berikut ini contoh yang penulis lakukan pada mesin Red Hat 9.0:

```
[root@syafii safii]# /sbin/
grub-md5-crypt
Password:
Retype password:
$1$1UogH0$cZpecMy.Ea0ue7vNBp/
Xk1
```

Password yang penulis gunakan adalah 6u4c4q3p!). Password tersebut akan di-enkripsi menggunakan algoritma md5 menjadi \$1\$1UogH0\$cZpecMy.Ea0ue7vNBp/Xk1. Ingat dengan benar password hasil enkripsi tadi.

3. Sebaiknya Anda salin file hasil enkripsi ke editor teks Anda, misal vi. Password yang telah terenkripsi ini akan kita masukkan ke dalam file konfigurasi GRUB. Buka grub.conf yang terletak di /boot/grub/ dengan perintah vi /boot/grub/grub.conf. Berikut ini isi file grub.conf yang sudah dimodifikasi:

```
default=1
timeout=10
password --md5
$1$1UogH0$cZpecMy.Ea0ue7vNBp/
Xk1
splashimage=(hd0,7)/boot/
grub/splash.xpm.gz
title Red Hat Linux (2.4.20-8)
    root (hd0,7)
    kernel /boot/vmlinuz-
2.4.20-8 ro root=LABEL=/
initrd /boot/initrd-
2.4.20-8.img
title Windows
    rootnoverify (hd0,0)
    chainloader +1
```

Tambahkan sebuah baris berikut di bawah baris "timeout=10":

```
password --md5
$1$1UogH0$cZpecMy.Ea0ue7vNBp/
Xk1
```

Format penambahannya yaitu:

```
password --md5 <password
yang sudah di enkripsi>.
```

Jika sudah Anda tambahkan, kemudian cek file permission file grub.conf. Gunakan perintah stat:

```
[safii@syafii safii]$ stat
/boot/grub/grub.conf
  File: `/boot/grub/grub.conf'
  Size: 673 Blocks: 8 IO B
lock: 4096 Regular File
Device: 308h/776d Inode:
261427 Links: 1
Access: (0600/-rw-----)
Uid: ( 0/ root) Gid:
( 0/ root)
Access: 2004-03-24
11:42:40.000000000 +0700
Modify: 2004-03-24
11:42:40.000000000 +0700
Change: 2004-03-24
11:42:40.000000000 +0700
```

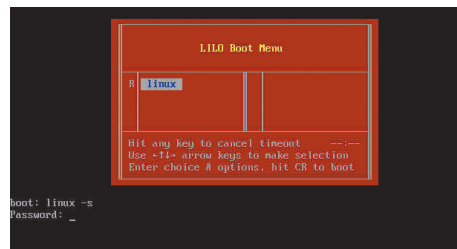
Pastikan file permissionnya 600, yang artinya file tersebut hanya dapat di baca dan diedit oleh root. Apabila file permission masih belum 600, gunakan perintah chmod:

```
[root@syafii grub]# chmod 600
grub.conf
```

4. Jika semua konfigurasi telah dilakukan dengan benar, reboot komputer Anda. Ketika GRUB tampil waktu booting, untuk masuk ke editor biasanya anda mengetikkan 'e' terlebih dahulu. Tapi karena sudah diberi password, Anda harus mengetikkan 'p' dahulu kemudian memasukkan password untuk masuk ke editor (Gambar 1).

Namun, pengamanan seperti di atas masih tidak cukup karena bisa saja masuk ke opsi booting yang lain yaitu masuk ke opsi Windows jika menggunakan dual boot. Untuk mengunci (lock) agar tidak dapat masuk ke Windows, maka buka lagi file grub.conf. Tambahkan kata 'lock' di bawah title Windows.

Reboot kembali pc Anda. Pada menu GRUB, pindah kursus ke Windows, maka proses booting akan berhenti sebelum anda menekan tombol 'p' pada GRUB dan mema-



Gambar 2. Password pada Lilo.

sukkan password. Jika anda hanya menamabahkan kata lock saja, maka untuk mengedit GRUB dan masuk Windows menggunakan password yang sama. Tetapi jika ingin memberikan password yang berbeda ketika ingin booting ke Windows, tambahkan baris lock dan password:

```
title Windows
lock
password --md5
$1$1UogH0$cZpecMy.Ea0ue7vNBp/Xk1
```

Untuk menghasilkan enkripsi password (dapat men-generate sendiri), ketikkan perintah:

```
# /sbin/grub-md5-crypt
```

Password pada LILO

1. Buka file /etc/lilo.conf.
2. Di bawah image=/boot/vmlinuz-<xx> tambahkan baris password:

```
password=password_anda
restricted
```

Arti restricted adalah: jika seseorang memasukkan perintah boot dengan menggunakan argumen ketika tampil boot prompt, maka dia harus memasukkan password terlebih dahulu. Misalnya mengetikkan 'linux -s' yang artinya login dengan linux single (Gambar 2).

Password pada Lilo bukan password terenkripsi. Anda harus atur agar permission-nya (atribut file) tidak bisa dilihat oleh user yang bukan root (pastikan bahwa atribut file lilo.conf adalah 600). Jangan lupa setelah melakukan perubahan pada lilo.conf jalankan perintah:

```
# /sbin/lilo -v
```

Catatan:

Keamanan BIOS dan boot loader bisa hilang, jika reset jumper atau cabut baterai CMOS. ☹

M Syafii (karebet_asli@telkom.net)