TBOOT Argument Measurement Vulnerability for ELF Kernels

JP Blake

As described on Intel's website, "Trusted Boot (tboot) is an open source, pre- kernel/VMM module that uses Intel® Trusted Execution Technology (Intel® TXT) to perform a measured and verified launch of an OS kernel/VMM."

One essential function TBOOT performs as part of a measured and verified launch includes measuring the arguments passed to GRUB modules. However, current versions of TBOOT used on systems loading an ELF kernel have a vulnerability that allows the first argument to any GRUB module to go unmeasured, which may result in undetected system compromise.

This vulnerability stems from TBOOT's "official" workaround for accommodating GRUB2 multiboot behavior. Specifically, from the TBOOT README:

```
GRUB2 does not pass the file name in the command line field of the multiboot
entry (module_t::string). Since the tboot code is expecting the file name as
the first part of the string, it tries to remove it to determine the command
line arguments, which will cause a verification error. The "official"
workaround for kernels/etc. that depend on the file name is to duplicate the
file name in the grub.config file like below:
menuentry 'Xen w/ Intel(R) Trusted Execution Technology' {
recordfail
insmod part_msdos
insmod ext2
set root='(/dev/sda,msdos5)'
search --no-floppy --fs-uuid --set=root 4efb64c6-7e11-482e-8bab-07034a52de39
multiboot /tboot.gz /tboot.gz logging=vga,memory,serial
module /xen.gz /xen.gz iommu=required dom0_mem=524288 com1=115200,8n1
module /vmlinuz-2.6.18-xen /vmlinuz-2.6.18-xen root=/dev/VolGroup...
module /initrd-2.6.18-xen.img /initrd-2.6.18-xen.img
module /Q35_SINIT_17.BIN
}
```

To illustrate the severity of the bug, consider that on affected distributions, it would be possible to edit a GRUB command line from:

```
module  /vmlinuz /vmlinuz normal-arguments
```

to:

```
module  /vmlinuz single normal-arguments
```

Where 'single' replaces the typical placeholder argument. This modification goes undetected by TBOOT and consequently the assertion that the system has been measured and verified is undermined. Namely, the final measurement shown in the TPM PCR-18 does not change to reflect the modification.

Some major distributions use ELF kernels and are affected:

Affected versions:	Unaffected versions:
Debian Wheezy	Ubuntu 12.04LTS, 14.04LTS
Citrix XenClientXT	Centos 6.x, 7.x
	Fedora 20

In summary, TBOOT makes assumptions and changes in behavior based on whether it is executing with GRUB Legacy or GRUB2. In the case where TBOOT loads an ELF kernel, this behavior results in an unmeasured argument being passed to the kernel. Regardless of the GRUB version and how arguments are handled by TBOOT, the most prudent action for TBOOT to take is to measure all command line arguments. The patch below illustrates that one way of modifying TBOOT to achieve this goal is a two line patch:

```
diff --git a/tboot-1.8.1/tboot/common/policy.c b/tboot-1.8.1/tboot/common/policy.c
index faed9e5..db0dcd1 100644
--- a/tboot-1.8.1/tboot/common/policy.c
+++ b/tboot-1.8.1/tboot/common/policy.c
@@ -424,8 +424,6 @@ static bool hash_module(hash_list_t *hl,
     /* hash command line */
     if ( cmdline == NULL )
         cmdline = "";
-    else
-        cmdline = skip_filename(cmdline);

     switch (g_tpm->extpol) {
     case TB_EXTPOL_FIXED:
```