Eirik Vestreng Solberg

120917

Obligatory exercise 1

2014-09-03

Trusted Path Windows RT (ARM Architecture)

Secure Attention Sequence first appeared in Windows in the NT kernel. By pressing this sequence, ctrl+alt+delete for example, it sends an interrupt to the kernel and makes it take over screen and showing the trusted path. This is also implemented on windows R/T thereby the both windows tablets such as Surface and Windows Phone. A question arises from this, is it still a trusted path in the ARM architecture?

The Architecture

ARM has seven modes of operation: user mode, fast interrupts FIQ, supervisor mode, abort mode, normal interrupt mode, system mode and undefined. User mode is the only non-privileged (1). Switching Between these modes is possible by altering the mode bits in the CPSR register (2)

ARM has several types of interrupt for different purposes. IRQ are used for normal interrupts with normal priority, FIQ purpose is almost like IRQ with the difference in the urgency and because of this FIQ has some dedicated registers for this in case of context before interrupt code execution. (3)

SWI are the interrupt used for normal calls to kernel and the supervisor and are used to put the CPU in SVC mode (4)

NMI (Non-Maskable Interrupt) is used to notify about serious errors or SAS (Secure Attention Sequence) (5). Notice in the figure how normal interrupts are stacked and NMI interrupts is non-interruptible.

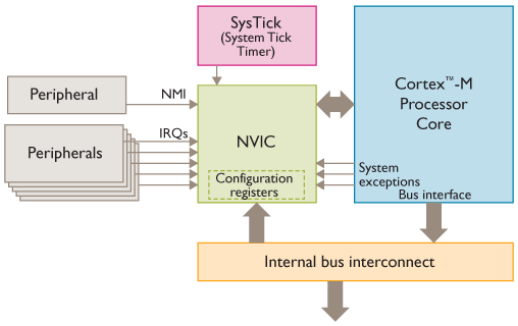

FIGURE 1: EXEMPLIFIED ARM INTERRUPT HANDLING

The Operating System

Windows RT uses a modified version of the NT kernel. Thereby have the trusted path incorporated. It is possible to turn of IRQ and FIQ interrupts in an application by altering some bits in the CPSR register (2). It is however not possible to stop other interrupts like NMI and SWI like this since both are used by the kernel (4).

Conclusion

Since windows RT uses a modified NT kernel it is reasonable to think that SAS is executed as an NMI interrupt which by definition should be un-interruptible and un-maskable. It is possible to invoke and NMI by application, so it is therefore possible to make a tile shortcut to invoke it. So by this given the scenario that the tile actually invoke the interrupt and not malicious code, the result will be a trusted path

References

1. **Kumar, Gaurav and Gupta, Aditya.** A Short Guide on ARM Exploitation. [Online] [Cited: 09 03, 2014.] http://www.exploit-db.com/wp-content/themes/exploit/docs/24493.pdf.

2. **Abdelrazek, Ahmed Fathy.** *Introducing ARM architeture.* s.l. : Univärsitet Stuttgart, 2013.

3. **ARM the Architecture for the digital world.** ARM the Architecture for the digital world. [Online] 09 03, 2014. http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.ddi0363g/BEIDDFBB.html.

4. **HeyRick.co.uk.** HeyRick.co.uk. [Online] [Cited: 09 03, 2014.] http://www.heyrick.co.uk/armwiki/Processor_modes.

5. **Computer Hope.** Computer Hope. [Online] [Cited: 09 03, 2014.]