Hardware/Software Support for Securing Virtualization in Embedded Systems

Franck BUCHERON[1,2], Arnaud TISSERAND[3,2] and Louis RILLING[1,2]

[1] DGA-MI
franck.bucheron | louis.rilling@intradef.gouv.fr
[2] IRISA – [3] CNRS – Univ. Rennes 1 – INRIA
arnaud.tisserand@cnrs.fr

Abstract. Up to some years ago, mainly high-performance processors, such as those in servers and desktops, were powerful enough to support *virtualization*. This was mainly used at software level to provide *isolation*, *security services* and *resources sharing*. Today, even processors for embedded systems can also efficiently support virtualization. But on top of isolation and protection against *software attacks*, embedded systems have also to face *hardware attacks* such as *side channel attacks* (SCAs). Hence, virtualization for embedded systems requires a combined *hardware/software (HW/SW) approach*.

In this paper, we first provide an important review and analyze state-of-art solutions. Then, we describe our own solution. we study an embedded virtualization solution based on HW IPs and a SW stack for efficiently protecting the system against SW attacks. Security against SCAs comes from the used of optimized and SCA-protected hardware IPs for primitives such as symmetric/asymmetric cryptography and true random number generation (TRNG). Using this hardware/software approach, we expect better performances, security and lower power consumption compared to software solutions. Our system is implemented in a Zynq-7000 HW/SW platform composed of a processor (ARM Cortex-A9 dual-core) and a FPGA (Artix-7) in the same device. For the SW stack, we use a derived version of the Xen hypervisor. In order to offer efficient, robust and low-power integrity, confidentiality and authentication primitives, we use a minimal list of existing HW IPs: AES (256 bits) for symmetric encryption/decryption, ECC (between 192 and 256 bits), RSA (2048 bits), TRNG, SHA-2 (256 bits). In addition to these HW IPs, we have to add a few other HW blocks: I/O interface between HW and SW, various internal memories (for PCRs and keys), control and execution engine (for the HW part of implemented security policies). At the SW level, we adapted a Xen-like hypervisor to our HW architecture. Our SW code links the various virtual machines (VMs), the management VM (Dom0) and the hardware architecture. The proposed HW architecture and SW stack allows the end user to launch VMs where the executed code is trusted (i.e. verified and the user is granted) and the manipulated data are also trusted (i.e. integrity is ensured and only authorized users have access to these data inside the complete HW/SW platform).

Keywords: TCG, TPM, ARM Cores, Virtualization, Embedded systems, Xen hypervisor, Xilinx

Documents cités :

[17] [18] [3] [11] [6] [5] [14] [23] [24] [4] [16] [13] [8] [15] [7] [12] [19] [20] [1] [2] [10] [22] [9] [21]

References

1. Aguiar, A., Hessel, F.: Embedded system's virtualization : The next challenge ? pp. 1–7 (2010), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5656430&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5656430
2. Coker, G., Guttman, J., Loscocco, P., Herzog, A., Millen, J., O'Hanlon, B., Ramsdell, J., Segall, A., Sheehy, J., Sniffen, B.: Principles on remote attestation. International Journal of Information Security 10, 63–81 (2010), http://link.springer.com/article/10.1007%2Fs10207-011-0124-7
3. Department of Defense, USA: Orange security book (1983), http://csrc.nist.gov/publications/history/dod85.pdf
4. England, P., Loeser, J.: Para-virtualized tpm sharing pp. 119–132 (2008), http://dx.doi.org/10.1007/978-3-540-68979-9_9
5. Nationale Institute of Standards and Technology: Guidelines on hardware-rooted security in mobile devices (draft) (2012), http://csrc.nist.gov/publications/PubsDrafts.html#SP800-164
6. Nationale Institute of Standards and Technology: Recommandation for key management : Part 1 : General (revision 3) (2012), http://csrc.nist.gov/nistpubs/800-57/sp800-57_part1_rev3.pdf
7. Osborn, J.D., Challenger, D.C.: Trusted platform module evolution. APL technical Digest 32 (2013), http://www.jhuapl.edu/techdigest/TD/td3202/32_02-Osborn.pdf
8. Parno, B., McCune, J.M., Perrig, A.: Bootstrapping trust in commodity computers (2013), https://sparrow.ece.cmu.edu/group/pub/PaMcPe2010.pdf
9. Pearce, M., Zeadally, S., Hunt, R.: Virtualization: Issues, security threats, and solutions. ACM Comput. Surv. 45(2), 17:1–17:39 (2013), http://doi.acm.org/10.1145/2431211.2431216
10. Pék, G., Buttyán, L., Bencsáth, B.: A survey of security issues in hardware virtualization. ACM Comput. Surv. 45(3), 40:1–40:34 (2013), http://doi.acm.org/10.1145/2480741.2480757
11. Ponsini, N.: Trusted embedded computing (2010), http://cordis.europa.eu/project/rcn/85362_en.html
12. Rossier, D.: Embeddedxen : A revisited architecture of the xen hypervisor to support arm-based embedded virtualization (2012), http://sourceforge.net/projects/embeddedxen/
13. Roth, T.: Next generation mobile rootkits (2013), https://www.hackinparis.com/sites/hackinparis.com/Slidesthomasroth.pdf

14. Sadeghi, A.R., Stble, C., , Winandy, M.: Property based tpm virtualization. In: 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18, 2008. pp. 1–16. Springer-Verlag, Berlin, Heidelberg (2008), http://link.springer.com/chapter/10.1007%2F978-3-570-85886-7_1#
15. Samsung Electronics Co, ltd: Secure xen on arm user's guide (2008), http://downloads.xenproject.org/Wiki/XenARM/Secure_Xen_on_ARM_User_Guide_v1_0.pdf
16. Smith, J.E., Nair, R.: Virtual machines. Elsevier (2005)
17. Stefan, B., Cáceres, R., Goldman, K.A., Perez, R., Sailer, R., van Doorn, L.: vtpm: Virtualizing the trusted platform module. In: Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15. USENIX-SS'06, USENIX Association, Berkeley, CA, USA (2006), http://dl.acm.org/citation.cfm?id=1267336.1267357
18. Stumpf, F., Eckert, C.: Enhancing trusted platform modules with hardware-based virtualization techniques. In: Proceedings of the Second International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2008, August 25-31, 2008, Cap Esterel, France. pp. 1–9 (2008), http://dx.doi.org/10.1109/SECURWARE.2008.23
19. Trusted Computing Group: Virtualized trusted platform architecture specification (2011), http://www.trustedcomputinggroup.org/resources/virtualized_trusted_platform_architecture_specification
20. Trusted Computing Group: Tpm mobile with trusted execution environment for comprehensive mobile device security (2012), http://www.trustedcomputinggroup.org/files/static_page_files/5999C3C1-1A4B-B294-D0BC20183757815E/TPM%20MOBILE%20with%20Trusted%20Execution%20Environment%20for%20Comprehensive%20Mobile%20Device%20Security.pdf
21. Trusted Computing Group: Credential_profile_ek_v2.0_r12_publicreview (2014), http://www.trustedcomputinggroup.org/files/static_page_files/DCD56924-1A4B-B294-D0CEF64E80CEE01E/Credential_Profile_EK_V2.0_R12_PublicReview.pdf
22. Waksman, A., Sethumadhavan, S.: Silencing hardware backdoors. In: Proceedings of the 2011 IEEE Symposium on Security and Privacy. pp. 49–63. SP '11, IEEE Computer Society, Washington, DC, USA (2011), http://dx.doi.org/10.1109/SP.2011.27
23. Xilinx: Secure boot of zynq-7000 all programmable soc (2013), http://www.xilinx.com/support/documentation/application_notes/xapp1175_zynq_secure_boot.pdf
24. Xilinx: Zynq-7000 all programmable soc secure boot (2014), http://www.xilinx.com/support/documentation/user_guides/ug1025-zynq-secure-boot-gsg.pdf