SDTA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000	0000000	00

Hardware/Software Support for Securing Virtualization in Embedded Systems

Franck Bucheron

IRISA-CAIRN DGA

December 4, 2014





SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000	0000000	00

Goal of this thesis

2 State-of-the-Art

- Hardware
- Virtualization
- Trusted computing
- Threats

3 Contribution

- Overall solution
- Boot and zynq-7000
- Virtual TPM



SDTA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000	0000000	00

Goal of this thesis

2 State-of-the-Art

- Hardware
- Virtualization
- Trusted computing
- Threats

3 Contribution

- Overall solution
- Boot and zynq-7000
- Virtual TPM

ConclusionTODO list

SDTA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
	•	00000000000	0000000	00
Goal of this thesis				
o Imp	rove the trust in virtu	alization for ARM em	bedded platforms.	
•			I.	
2 Mo	dify studied propositio	ns add new ideas to	build a functionnal v	/irtual

embedded system as secure as possible.

SDTA-20	14 Introduction	State-of-the-Art 000000000000	Contribution 0000000	Conclusion
Goal of th	is thesis			
	Improve the trust in virt	ualization for ARM em	bedded platforms.	
	Modify studied propositions, add new ideas to build a functionnal virtual embedded system as secure as possible.			irtual
	Starting point: conside	r that embedded syste virtualization	ms efficiently suppor	t
U	se a combined <i>hardware/so</i>	ftware (HW/SW) appr	oach, with:	
	Implementation on a Zyn dual-core) and a FPGA	nq-7000 HW/SW platf (Artix-7),	orm (ARM Cortex-A	9
	e-use of existing HW c	ryptographic IPs,		
	Addition a few other HV	V blocks: TPM and vT	PM,	
	At the SW level, adaptat	tion of a Xen-like hype	rvisor to our HW	

architecture.

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion

Goal of this thesis

2 State-of-the-Art

- Hardware
- Virtualization
- Trusted computing
- Threats

Contribution

- Overall solution
- Boot and zynq-7000
- Virtual TPM

ConclusionTODO list

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		○○ ○○○○○○○○○		
Hardware				

Four different domains:

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		• 0 0000000000		
Hardware				

Four different domains:

- Hardware,
- 2 Existing software virtualization solutions in the open-source world,
- Concepts of trusted computing,
- O Threats.

SDTA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000		
Hardware				

FPGA and ASIC: No more opposition between with these 2 technologies.

To prototype hardware, only FPGA is relevant:

- Dynamicaly reconfigurable,
- 2 Can keep the configuration if in flash mode,

SDTA-2014 Introduction		State-of-the-Art	Contribution	Conclusion	
0 0 00000000 000000 000000 00000000000			00		
Hardv	vare				
	EDCA an	d ASIC: No mo	o opposition botwoon with	th those 2 technole	rior
	PGA and ASIC. No more opposition between with these 2 technologies.				
	To prototype	برامر متوبيرامترموا	EDCA is relevant.		
	To prototype	nardware, only	FPGA is relevant:		
	Demonstrative second investigation				
	Uynamically recomputable,				
	• Can keen the configuration if in flack mode				
	🕤 Can kee	p the configura	non n nash mode,		

To prototype software, only ASIC is relevant:

- Standard technology optimized,
- Performances.

SD	TA-2014 Introduction	State-of-the-Art	Contribution	Conclusion
	0	00000000000	0000000	00
Har	dware			
	EDCA and ASIC: No.	more ennecition between w	the three O toohnold	a mino
	FPGA and ASIC: No	more opposition between w	ith these 2 technolo	ogies.
	To prototype hardware	only EPGA is relevant:		
	ie piecespe natatiale, s			
	Oynamicaly reconfigure	gurable,		
	On keep the config	uration if in flash mode		
		diation in mash mode,		
	To prototype software, only ASIC is relevant:			
		·		
	Standard technology	y optimized,		
	2 Performances			

Hybrid platforms

Get avantages of the two types of circuits, plus:

- No extra daughter card needed,
- Shared peripherals if needed,
- Imagination required.

SDTA	-2014	Introduction O	State-of-the-Art ○○●○○○○○○○○○	Contribution 0000000	Conclusion 00
Virtua	lization				
		Few open-s	source hypervisors for	ARM cores	
			Review:		
	Nom		Pros	Cons	
					► = •940

SDTA-2014	Introduction O	State-of-the-Art ○○●○○○○○○○○○	Contribution 0000000	Conclusi 00
Virtualization				
	Few oper	n-source hypervisors for Al	RM cores	
		Review:		
Nom		Pros	Cons	
SierraViso	r	-paravirtualization -full hardware virtual- ization	-Zynq-7000 version closed source	is

SDTA-2014	Introduction O	State-of-the-Art ○○●○○○○○○○○○	Contribution 0000000	Conclus
Virtualization				
	Few open	-source hypervisors for Al	RM cores	
		Review:		
Nom		Pros	Cons	_
SierraVisor		-paravirtualization -full hardware virtual- ization	-Zynq-7000 version is closed source	
Xtratum		-allowing to run RTOS or real-time executives	-difficult to get the source code -don't run on Zynq- 7000	

SD TA-2014	Introduction O	State-of-the-Art ○○●○○○○○○○○○	Contribution	Conclusi
Virtualization				
	Few ope	n-source hypervisors for Al Review:	RM cores	
Nom		Pros	Cons	
SierraViso	r	-paravirtualization -full hardware virtual- ization	-Zynq-7000 version is closed source	;
Xtratum		-allowing to run RTOS or real-time executives	-difficult to get the source code -don't run on Zynq- 7000	
Xen ARM		-Xen ARM PV project	-no port on Zynq-7000	

SD TA-2014	Introduction O	State-of-the-Art ○○●○○○○○○○○○	Contribution	Conclus
Virtualization				
	F			
	Few ope	n-source hypervisors for Al	RIVI cores	
Review:				
Nom		Pros	Cons	
Sierra	/isor	-paravirtualization -full hardware virtual- ization	-Zynq-7000 version is closed source	
Xtratu	m	-allowing to run RTOS or real-time executives	-difficult to get the source code -don't run on Zynq- 7000	
Xen Al	RM	-Xen ARM PV project -Xen ARMv7+ project	-no port on Zynq-7000	
x-hyp		-ARINC like schedul- ing -reduced trusted base	-runs only on Qemu	

SD TA-	2014	Introduction	State-of-the-Art	Contribution	Conclusio 00
Virtuali	zation				
		Fow one	a source hypervisors for Al		
			Review:		
	Nom		Pros	Cons	
	SierraVisor		-paravirtualization -full hardware virtual- ization	-Zynq-7000 version is closed source	
	Xtratum		-allowing to run RTOS or real-time executives	-difficult to get the source code -don't run on Zynq- 7000	
	Xen ARM		-Xen ARM PV project -Xen ARMv7+ project	-no port on Zynq-7000	
	x-hyp		-ARINC ike schedu - ing -reduced trusted base	-runs only on Qemu	
	Embedded	Xen	-source code available -runs on a Zynq-7000 platform	-Current limitation to 1 domU	

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000000000000		
Trusted computing				

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000000000000		
Trusted computing				

- Trusted Computing Base
 - Set of all hardware, software and procedural components that enforce the security policy,
 - Must be as small as possible.

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000000000000		
Trusted computing				

- Trusted Computing Base
 - Set of all hardware, software and procedural components that enforce the security policy,
 - Ø Must be as small as possible.
- Irusted Platform Module (TPM) current version 2.0
 - Hardware component that provides a set of fixed cryptographic and security functions,
 - (Originally) intended to be platform independant.

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000000000000		
Trusted computing				

- Trusted Computing Base
 - Set of all hardware, software and procedural components that enforce the security policy,
 - Ø Must be as small as possible.
- **2** Trusted Platform Module (TPM) current version 2.0
 - Hardware component that provides a set of fixed cryptographic and security functions,
 - (Originally) intended to be platform independant.
- Irusted Software Stack (TSS)
 - Issues low-level TPM commands and receives low-level TPM responses on behalf of high-level applications,
 - (Originally) intended to be platform independant.

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000		
Trusted computing				

Some studies (mostly dedicated to x86) tried to solve the problem.

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000000000000		
Trusted computing				

Some studies (mostly dedicated to x86) tried to solve the problem.

vTPM: Virtualizing the Trusted Platform Module by Stefan Berger, 2006

Advantages : High fidelity to TCG specifications, no hardware constraints. Disadvantges : Weak strengh face to hardware or software attack, increase of TCB, hard to implement.



SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000		
Trusted computing				

Some studies (most dedicated to x86) tried to solve the problem.

Enhancing Trusted Platform Modules with Hardware-Based Virtualization Techniques by Frederic Stumpf, 2008

Advantages : Stronger.

 $\mathsf{Disadvantges}$: Many swap of context in the CPU, exclusively on x86 architecture.



SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000		
Trusted computing				

Some studies (most dedicated to x86) tried to solve the problem.

Para-Virtualized TPM Sharing by Paul England, 2008

Advantages : All is done in the VMM, scheduled access to TPM. Disadvantges : Weak strengh face to HW/SW attack, increase of TCB, hard to implement.



SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000000000000		
Trusted computing				

boot: confusion about definitions

Need a boot that proves to deliver more than a secure initial state.

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000 000 00000		
Trusted computing				

boot: confusion about definitions

Need a boot that proves to deliver more than a secure initial state.

authenticated Boot	secure Boot
Passive method	Active method
Integrity measures are stored	Proof to the system is existen-
securely	tial
Provides proof to a third party	Unable to prove configuration
via attestation	to a third party
Require a TPM	Do not require a TPM

SDTA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000 0000 0000		
Trusted computing				

boot: confusion about definitions

Need a boot that proves to deliver more than a secure initial state.

authenticated Boot	secure Boot
Passive method	Active method
Integrity measures are stored	Proof to the system is existen-
securely	tial
Provides proof to a third party	Unable to prove configuration
via attestation	to a third party
Require a TPM	Do not require a TPM



Figure: trusted boot = secure boot + authenticated boot

▲□▶ ▲□▶ ★ □▶ ★ □▶ - □ - つくぐ

SDTA	-2014 Introduction	State-of-the-Art	Contribution	Conclusion
_	0	000000000000000000000000000000000000000	0000000	00
Threa	S			
		Hardware threats		
	At lower level, main goal is t	to counterfeit the IP or I	C, steal or copy it.	
			1	
	🔮 Backdoor in hardware (solution: have its own to	ounary),	
	A Hardware vulnerability (solution: undate hardwa	are)	
		Solution. apaate haldwa	ne),	

(2) Hardware assisted malware (solution: develop antivirus software).

SDTA	2014 Introduction	State-of-the-Art	Contribution	Conclusion
Thursday	0	000000000000000000000000000000000000000	0000000	00
Inrea	8			
		mardware inreals		
	At lower level, main goal is	to counterfeit the IP or I	C, steal or copy it.	
	Backdoor in hardware	(solution: have its own fo	oundry),	
	e Hardware vulnerability	(solution: update hardwa	are),	

③ Hardware assisted malware (solution: develop antivirus software).



Figure: How to exploit

SDTA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000000000000000000000000000000000000000		
Threats				

Software threats

On virtualization (DOS, escalation of privilege or acquire information)

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusio
		0000000000000	0000000	00
Threats				
		Software threats		
		Software threats		
Or	virtualization (DOS, esca	alation of privilege or ac	quire information)	
•	 Compromise the guest (guest, Managment VM 	(guest to guest, internet to guest),	to guest, VM migr	ation to
¢	•			
C				
_				



Figure: from A Survey of Security Issues in Hardware Virtualization - 2013

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		000000000000000000000000000000000000000		
Threats				

Software threats

Compromise virtualization making DOS, try escalation of privilege or acquire information...

0

3

Ompromise the host OS (guest to host, internet to host, host to the self),



Figure: from A Survey of Security Issues in Hardware Virtualization - 2013

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000		
Threats				

Software threats

Compromise virtualization making DOS, try escalation of privilege or acquire information...

0

2

 Compromise the hypervisor (guest to hypervisor, host OS to hypervisor, Physical/Physical Management Interface to Hypervisor),



Figure: from A Survey of Security Issues in Hardware Virtualization - 2013

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000	000000	00

• Goal of this thesis

2 State-of-the-Art

- Hardware
- Virtualization
- Trusted computing
- Threats

3 Contribution

- Overall solution
- Boot and zynq-7000
- Virtual TPM

ConclusionTODO list

SD TA-	2014	lı C	ntroduction	S1	tate-of-the-Ar	t 00	Contribution ••••••	Conclusion 00
Overall	soluti	on						
	٥	Run on AF	RM cores with	no vir	tualizatio	n extensior	ıs,	
	2	Adapt the	solution to a c	dedicat	ted platfo	rm (Zynq-	7000),	
	3	Respect th	e basis of TCO	G com	pability fo	or TPM an	dvTPM.	J
	_	ſ				`		
			Dom0	DomT	(M1	VMx		
			TSP	TDD, TCS,	TSP	TSP	PS	
				Нуре	erviseur			

PL
 Unidirectionnal Double communication bus : one for requests and one for answers
 Unidirectionnal communication bus
 Parts of the TSS and the scheduler placed here to avoid an
 anagment of the TSB and sc compromize Dom0.

Figure: A leigthweight hypervisor of Xen type with VM looking for trust in an FPGA implemented TPM/vTPM

SD TA-2014	Introduction O	State-of-the-Art 000000000000	Contribution ○●○○○○○	Conclusion 00
Boot and zynq-7000				
	Pro	blem of the chain of tr	ust	
	7 7000 ()			

- The Zynq-7000 offered us only a secure boot
- O The AES-256 engine and the hash of the RSA public key are hard coded in Zynq
- O Possibility to change keys and use efuse or BBRAM.



Figure: from AVNET - x-fest2014

SDTA-2014	Introduction	State-of-the-Art	Contribution	Conclusion			
		00000000000	000000	00			
Boot and zynq-7000							
	Implomo	atation of a measured c	auonco				
	Implementation of a measured sequence						

Fill the gap between secure boot and launch of VM.

- Nothing can be done with stage-0 boot,
- With FSBL : TPM/vTPM bitstream,
- With SSBL : U-BOOT, VMM and VM.



SDTA	-2014	Introduction O	State-of-the-Art 000000000000	Contribution	Conclusion		
Virtua	і трм						
	TPM and vTPM provide the same services						
	The I/O interface will only manage the requests/answers from the DomT and the ID of the requester,						
	O The execution engine of the IP will be the central point of execution,						
	٥	Partial reconfiguration w crypto engines).	vill be implemented for	large body of logic	(typical		

▲□▶ ▲□▶ ▲目▶ ▲目▶ 目 のへぐ

SDTA	-2014	Introduction	State-of-the-Art 000000000000	Contribution	Conclusion	
Virtua	ТРМ					
TPM and vTPM provide the same services						
 The I/O interface will only manage the requests/answers from the DomT and the ID of the requester, 						

- ② The execution engine of the IP will be the central point of execution,
- Partial reconfiguration will be implemented for large body of logic (typical crypto engines).



Figure: heart of the TPM/vTPM →

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
			0000000	
Virtual TPM				

$\mathsf{Dom}\mathsf{T}$

- Will have a part of the TSS (TDD and TCS commands),
- Will schedule and verify the requests (from the VMs TSP) and route the answers,
- O Later : will sign requests to the TPM.

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
			0000000	
Virtual TPM				

DomT

- Will have a part of the TSS (TDD and TCS commands),
- Will schedule and verify the requests (from the VMs TSP) and route the answers,
- Later : will sign requests to the TPM.



SDTA	2014	Introduction O	State-of-the-Art 000000000000	Contribution	Conclusion	
Virtua	ТРМ					
1	Managment	: of kevs from v	TPM: Virtualizing the T	rusted Platform M	odule -	
	0		2006			
			2000			
	Will be inspired from S. BERGER,					
	 Independent key hierarchy per vTPM instance, 					

O AIK of vTPM signed by AIK of the hardware TPM for commodity.



- **1** Will be inspired from S. BERGER,
- Independent key hierarchy per vTPM instance,
- **O** AIK of vTPM signed by AIK of the hardware TPM for commodity.



SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
			000000	
Virtual TPM				
Hypervisor				

Need for new hypervisor functionnalities

- Add DomU (for our DomT at least) and ID for VM
- 2 Add new syscalls
- Modify source files

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
			000000	
Virtual TPM				
Hypervisor				

Need for new hypervisor functionnalities

- Add DomU (for our DomT at least) and ID for VM
- 2 Add new syscalls
- Modify source files



Figure: from EmbeddedXEN: A Revisited Architecture of the XEN hypervisor to support ARM-based embedded virtualization - 2012

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
		00000000000	0000000	00

Goal of this thesis

2 State-of-the-Art

- Hardware
- Virtualization
- Trusted computing
- Threats

3 Contribution

- Overall solution
- Boot and zynq-7000
- Virtual TPM



SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
				•0
TODO list				

A lot of work has to be done

- Produce the IP (TPM first, vTPM second),
- 2 Plug the re-used IPs, link them,
- Modify the hypervisor,
- Improve the security of implementation,
- Test and debug.

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
				•0
TODO list				

A lot of work has to be done

- Produce the IP (TPM first, vTPM second),
- 2 Plug the re-used IPs, link them,
- Modify the hypervisor,
- Improve the security of implementation,
- Test and debug.

Some other future options

- IP updates,
- Migration of VMs,
- o parallelism,
- Use of TZ (for the DomT ?)

SD TA-2014	Introduction	State-of-the-Art	Contribution	Conclusion
				00
TODO list				

Thanks for your attention



All the reference to the figures can be found on the joined article.