
CoCoTPM: Trusted Platform Modules for Virtual Machines in Confidential Computing Environments

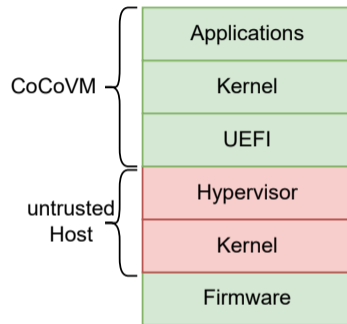
Joana Pecholt and Sascha Wessel, December 9, 2022



Background

Confidential Computing

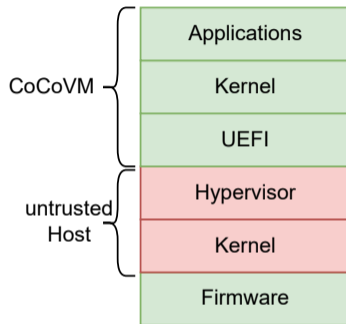
- Processing of sensitive data in the cloud
- Cloud provider is not trusted



Background

Confidential Computing

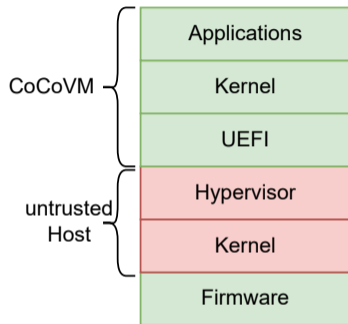
- Processing of sensitive data in the cloud
- Cloud provider is not trusted
- Minimal functionality of Confidential Computing
 - Protect data at rest, in use and in transit
 - Remote attestation



Background

Confidential Computing

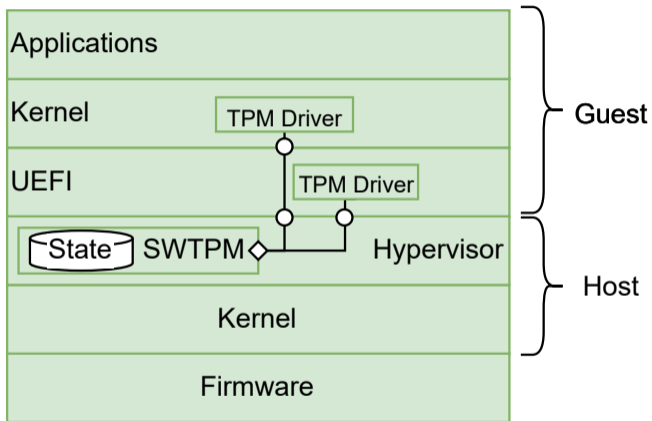
- Processing of sensitive data in the cloud
- Cloud provider is not trusted
- Minimal functionality of Confidential Computing
 - Protect data at rest, in use and in transit
 - Remote attestation



Challenge: Differing APIs for each confidential computing technology and limited functionality: AMD SEV-SNP, Intel TDX, Arm CCA

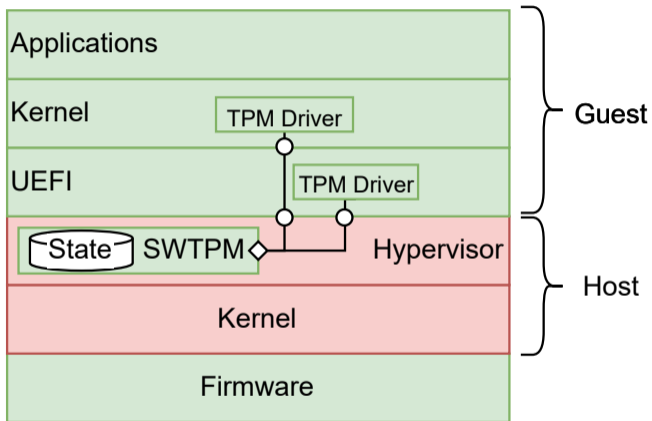
Background

Software TPMs



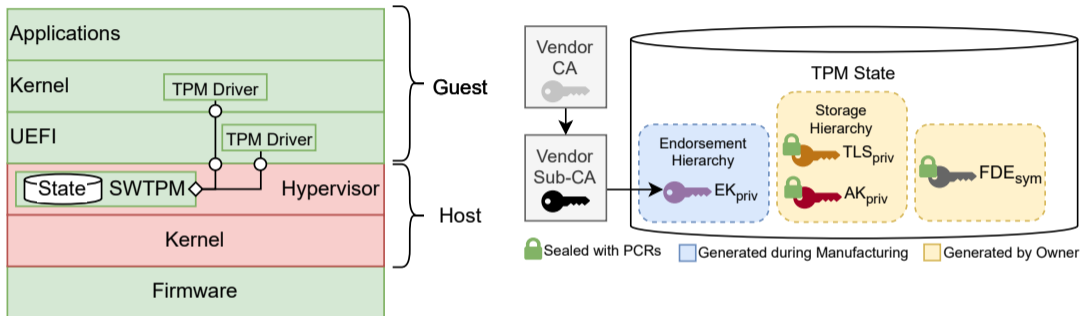
Background

Software TPMs



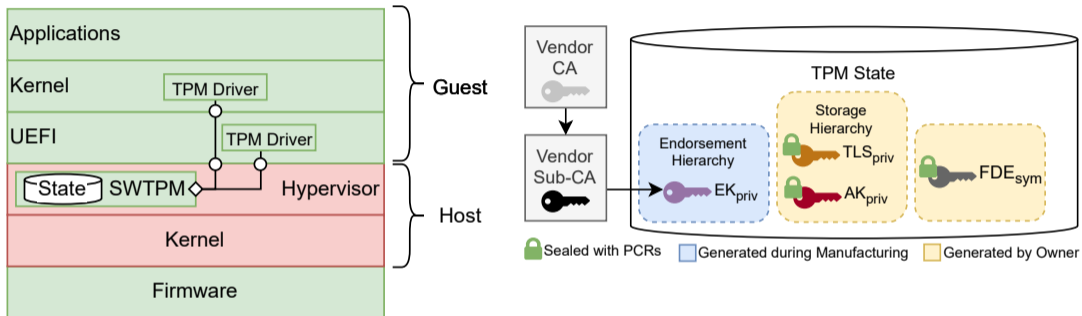
Problem

Software TPMs in Confidential Computing Environments



Problem

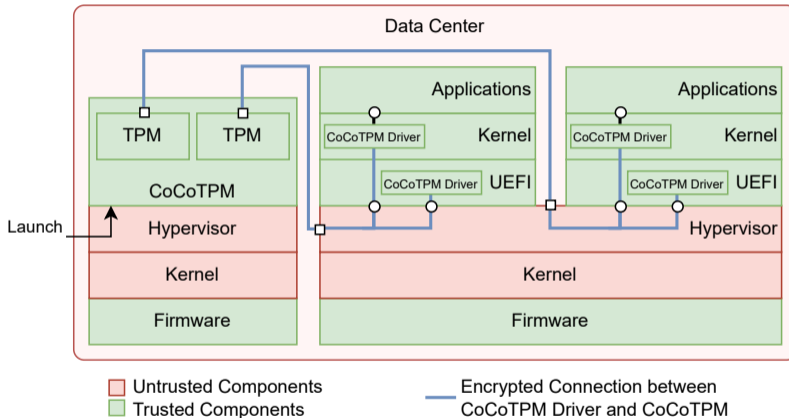
Software TPMs in Confidential Computing Environments



Challenges: Secure deployment, communication, persistent storage

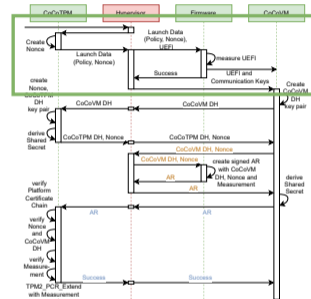
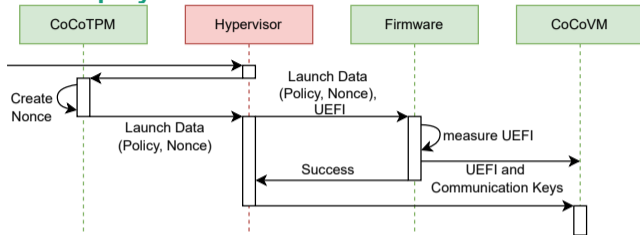
Concept

Overall System Architecture



Concept

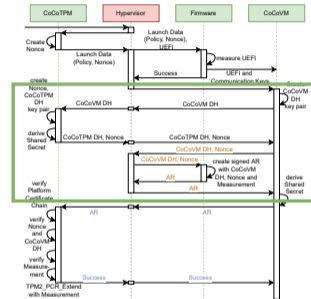
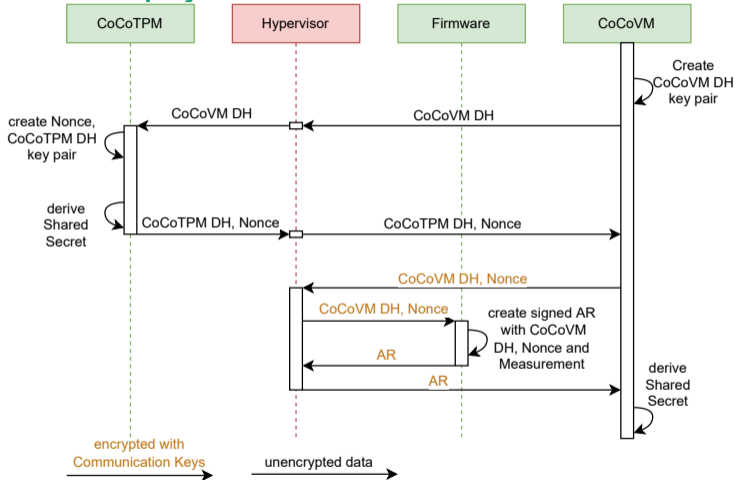
CoCoVM Deployment



unencrypted data →

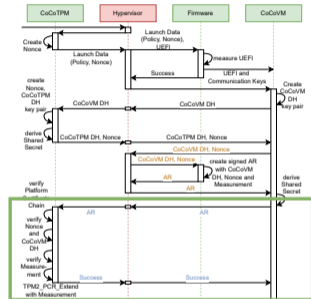
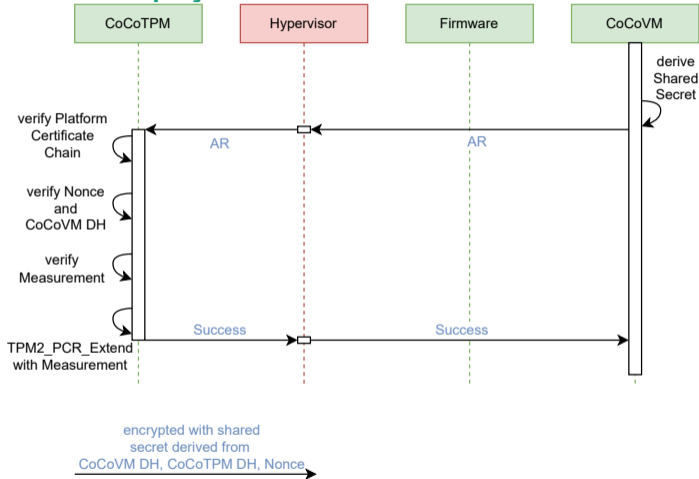
Concept

CoCoVM Deployment



Concept

CoCoVM Deployment



Concept

CoCoTPM Commands and Responses

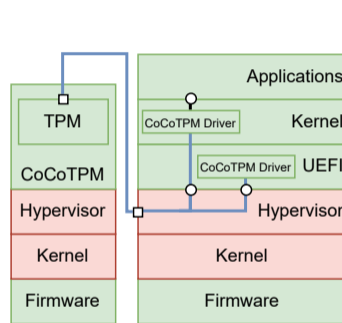
TPM Command

tag	length	command code	data
-----	--------	--------------	------

TPM Response

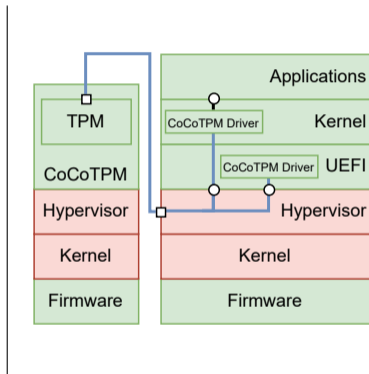
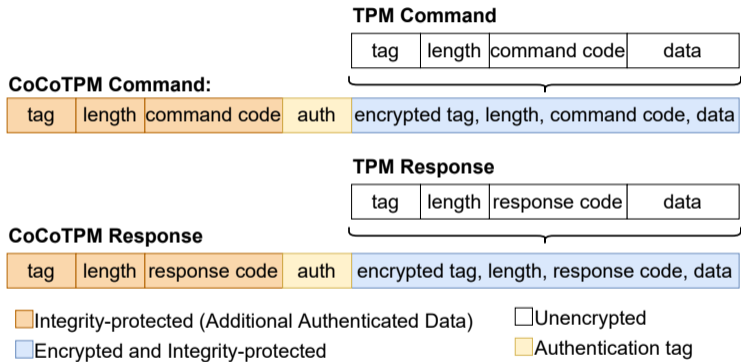
tag	length	response code	data
-----	--------	---------------	------

Unencrypted



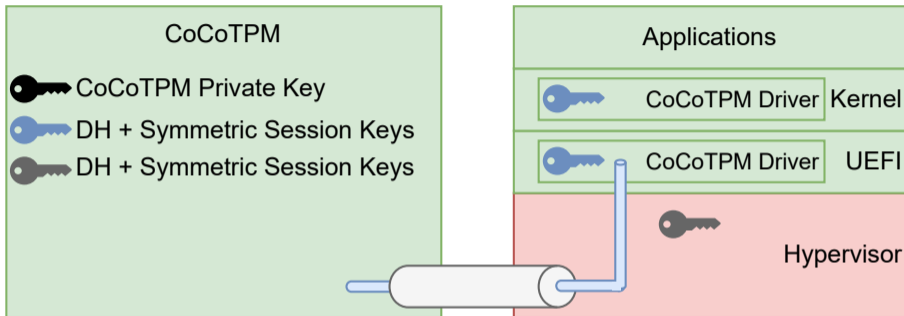
Concept



CoCoTPM Commands and Responses



Concept

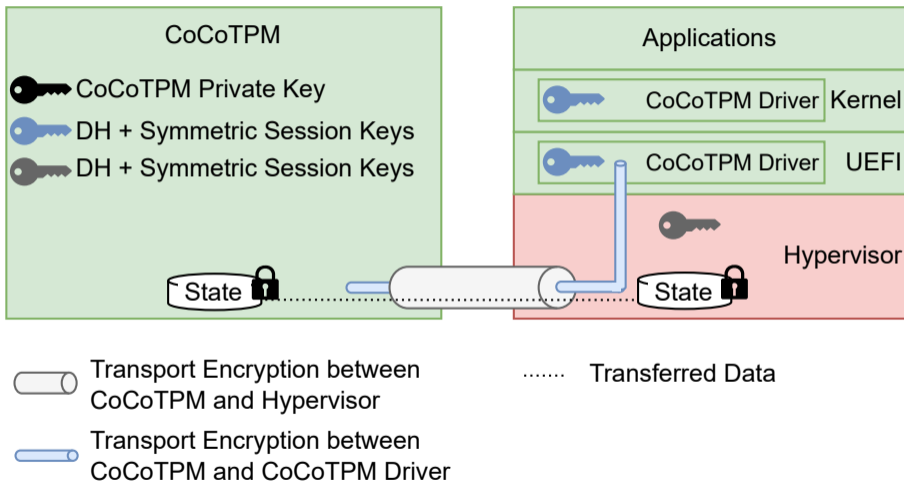
CoCoTPM Keys and Storage



-  Transport Encryption between CoCoTPM and Hypervisor
-  Transport Encryption between CoCoTPM and CoCoTPM Driver

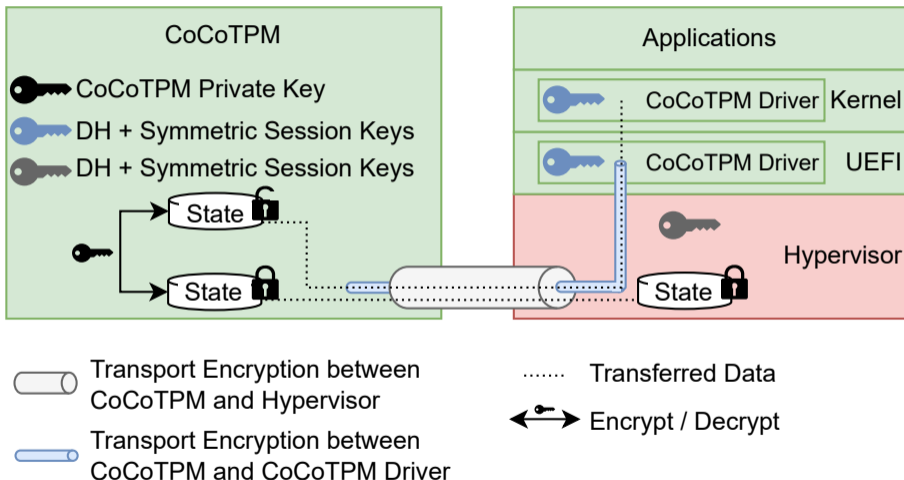
Concept

CoCoTPM Keys and Storage



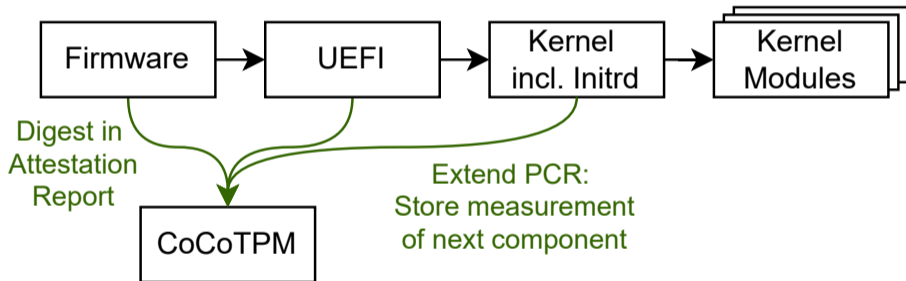
Concept

CoCoTPM Keys and Storage



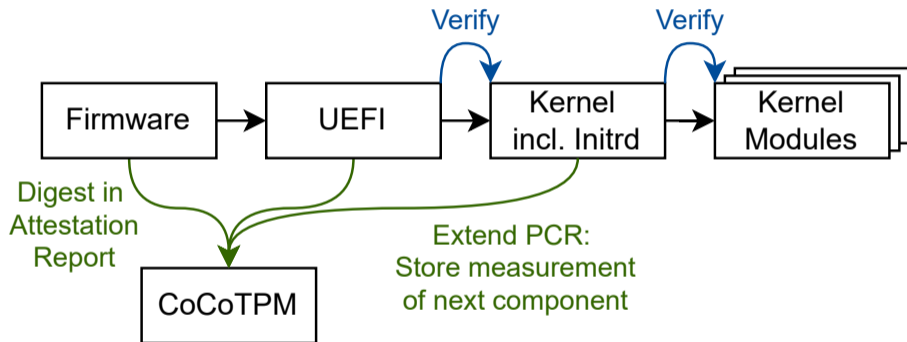
Concept

CoCoTPM Usage



Concept

CoCoTPM Usage



Concept

CoCoTPM Usage

- Authentication for communication:
 - TLS key stored inside CoCoTPM sealed to PCRs
 - Key usage only possible if CoCoVM booted into expected state

Concept

CoCoTPM Usage

- Authentication for communication:
 - TLS key stored inside CoCoTPM sealed to PCRs
 - Key usage only possible if CoCoVM booted into expected state
- Confidentiality and integrity protection of data at rest
 - Disk encrypted and integrity-protected
 - FDE key sealed to PCRs
 - Decryption of disk performed in CoCoVM only

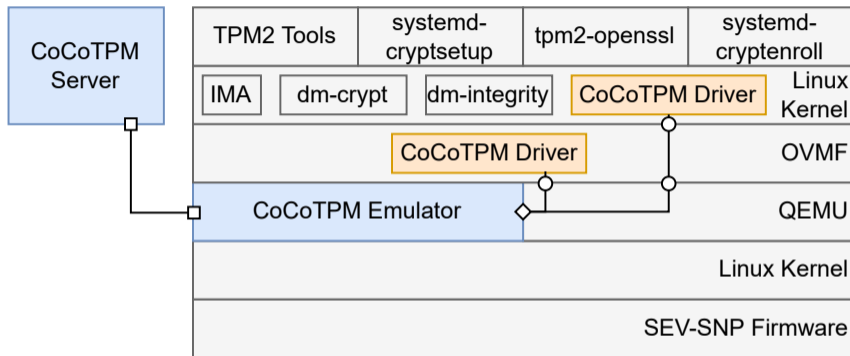
Concept

CoCoTPM Usage

- Authentication for communication:
 - TLS key stored inside CoCoTPM sealed to PCRs
 - Key usage only possible if CoCoVM booted into expected state
- Confidentiality and integrity protection of data at rest
 - Disk encrypted and integrity-protected
 - FDE key sealed to PCRs
 - Decryption of disk performed in CoCoVM only
- Remote attestation using CoCoTPM
 - TPM quotes as part of remote attestation
 - CoCoTPM attests hardware-specific software and components

Implementation

Proof of Concept



◇ Unix Domain Socket

□ TCP/IP Socket

○ System/Hypervisor Call / IO

◻ Modified existing components

◻ Implemented using existing components

◻ Newly implemented

Evaluation

Protocol size and execution times

	# TPM Cmds	received / transmitted bytes				execution time in milliseconds									
		TPM		CoCoTPM		dTPM		fTPM			SWTPM			CoCoTPM	
		RX	TX	RX	TX	NTC	IFX	INTC	QEMU	SEV	SNP	SEV	SNP		
tpm2_hash sha256 1kb	2	1054	136	1124	212	22	39	11	5	6	8	10	14		
tpm2_getrandom 32b	3	46	451	142	558	25	23	11	5	5	6	12	16		
tpm2_pcrread sha256 0-23	5	94	963	274	1122	31	24	16	8	8	10	19	27		
tpm2_create rsa2048	20	5398	6058	5992	6680	3653	12557	4925	83	93	119	151	189		
tpm2_create ecc256	20	5398	5770	5992	6392	219	1020	160	44	47	64	94	144		
tpm2_sign sha256 rsa2048	32	8716	9267	9616	10208	295	1615	397	72	76	103	152	219		
tpm2_sign sha256 ecc256	32	4716	4885	5616	5824	245	1245	308	53	55	69	131	206		
tpm2_encryptdecrypt aes128 1kb	26	4723	4805	5476	5588	140	680	150	47	48	63	109	189		

Evaluation

Protocol size and execution times

	# TPM Cmds	received / transmitted bytes				execution time in milliseconds									
		TPM		CoCoTPM		dTPM		fTPM			SWTPM			CoCoTPM	
		RX	TX	RX	TX	NTC	IFX	INTC	QEMU	SEV	SNP	SEV	SNP		
tpm2_hash sha256 1kb	2	1054	136	1124	212	22	39	11	5	6	8	10	14		
tpm2_getrandom 32b	3	46	451	142	558	25	23	11	5	5	6	12	16		
tpm2_pcrread sha256 0-23	5	94	963	274	1122	31	24	16	8	8	10	19	27		
tpm2_create rsa2048	20	5398	6058	5992	6680	3653	12557	4925	83	93	119	151	189		
tpm2_create ecc256	20	5398	5770	5992	6392	219	1020	160	44	47	64	94	144		
tpm2_sign sha256 rsa2048	32	8716	9267	9616	10208	295	1615	397	72	76	103	152	219		
tpm2_sign sha256 ecc256	32	4716	4885	5616	5824	245	1245	308	53	55	69	131	206		
tpm2_encryptdecrypt aes128 1kb	26	4723	4805	5476	5588	140	680	150	47	48	63	109	189		

↓
+13%

↓
performance between
dTPM / SWTPM

Conclusion

- Overall system architecture providing TPM functionalities to CoCoVMs excluding the hypervisor and operator / admin from the TCB
- Applying TPM functionalities to address common requirements in confidential computing environments for
 - Secure boot and measured boot
 - Confidentiality and integrity for data at rest
 - Authentication for communication
 - Remote attestation of VMs including their runtime state
- Architecture and protocols providing the following features
 - Protection of the TPM code and data against the host and its operator
 - Storage of runtime integrity measurements during measured boot and for the IMA
 - Unified format for remote attestation
 - Addressing attack vectors including replay attacks and reset attacks
- PoC for AMD SEV and AMD SEV-SNP and evaluation

Contact Information



Joana Pecholt

Department
Secure Operating Systems

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Lichtenbergstr. 11
85748 Garching (near Munich)
Germany

Internet: <http://www.aisec.fraunhofer.de>

E-Mail: joana.pecholt@aisec.fraunhofer.de