Securing the Distribution and Storage of Secrets with Trusted Platform Modules

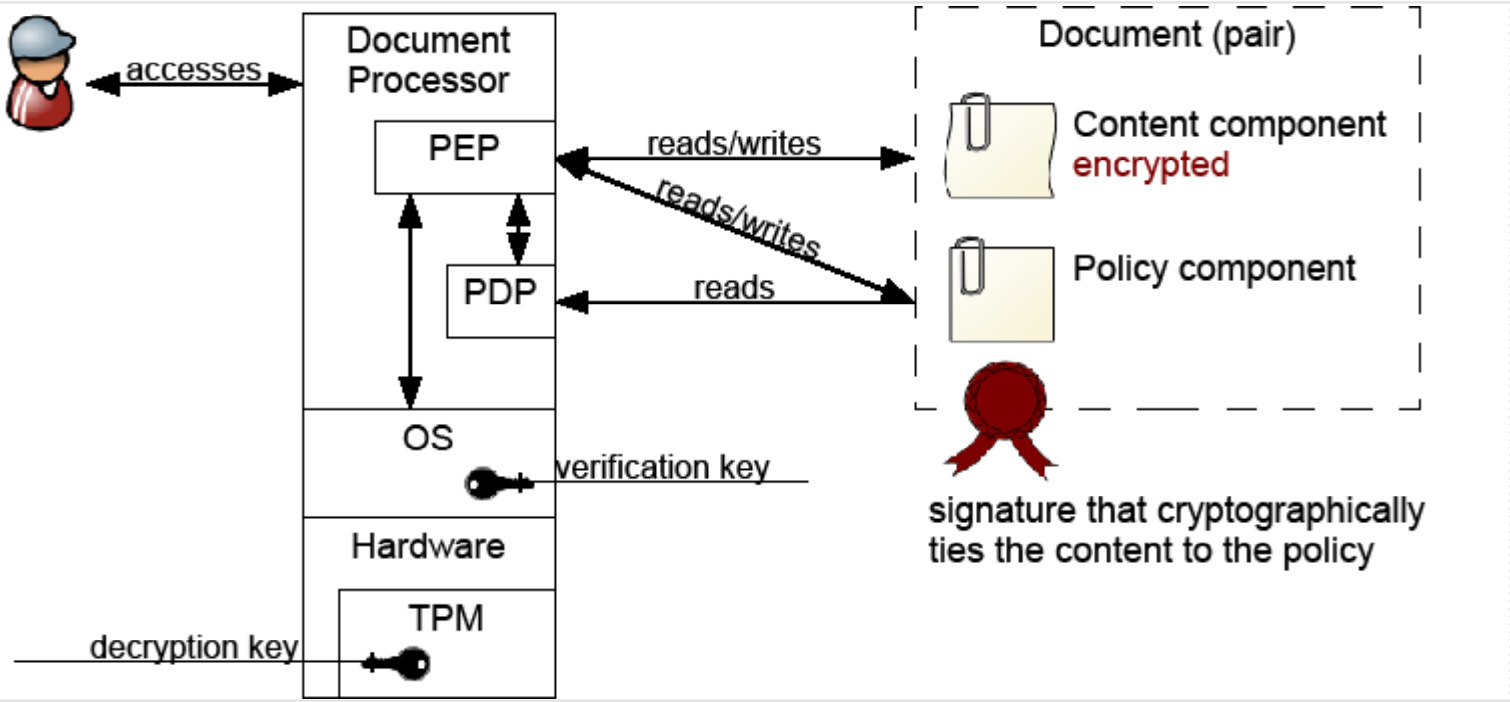
Paul E. Sevinç, Mario Strasser, and David Basin

ETH Zürich, Switzerland

Contents

- Motivation
- Background
- Requirements
- Protocol
- Security Analysis
- Conclusion

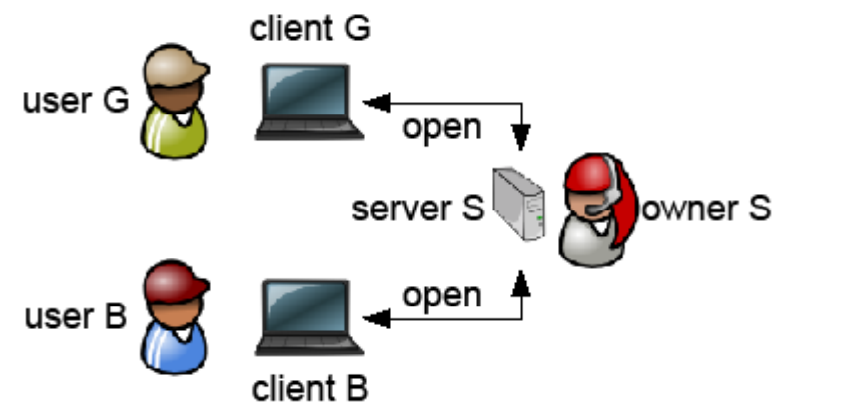
Motivation


accesses
Document Processor
PEP
PDP
OS
Hardware
TPM
reads/writes
reads/writes
reads
verification key
decryption key
Document (pair)
Content component
encrypted
Policy component
signature that cryptographically ties the content to the policy

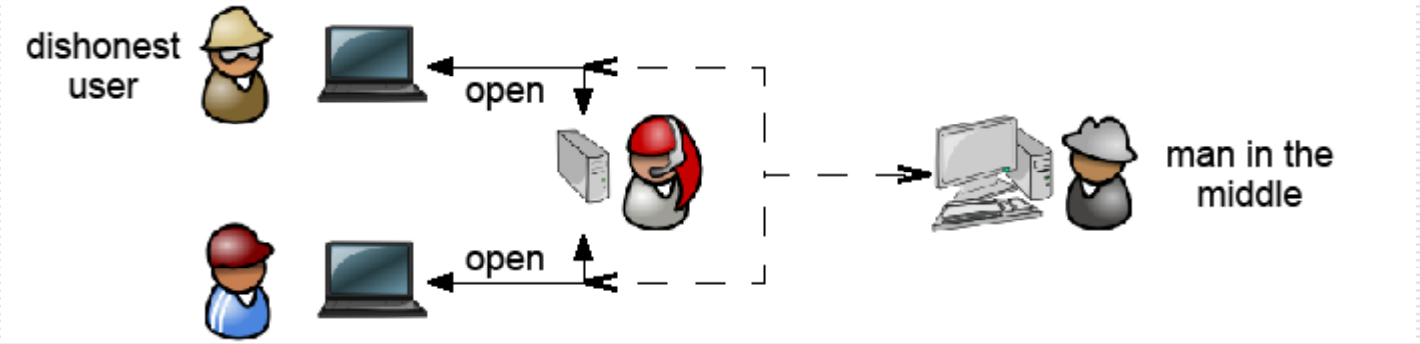
Background

- Trusted Computing based on three so-called Roots of Trust:
  - Root of Trust for Measurement (RTM)
  - Root of Trust for Reporting (RTR)
  - Root of Trust for Storage (RTS)
- BIOS: RTM (not tamper-resistant)
- Trusted Platform Module (TPM): RTR & RTS (not tamper-proof)

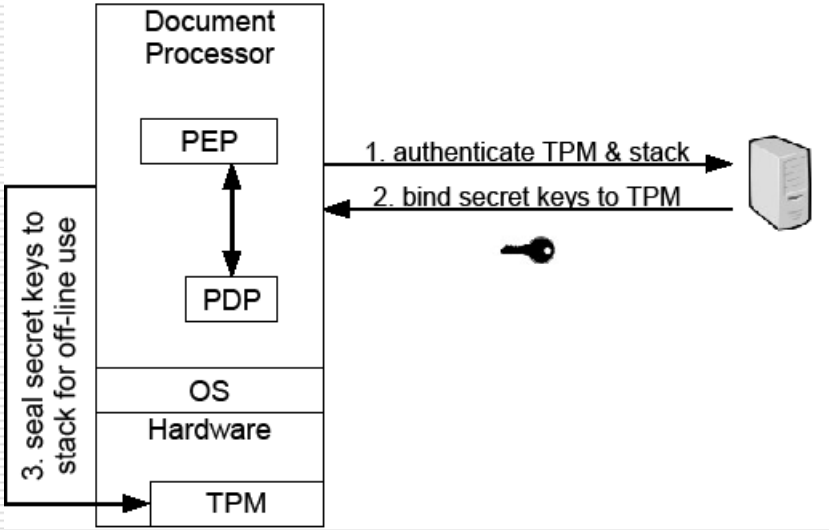
Requirements: Setting



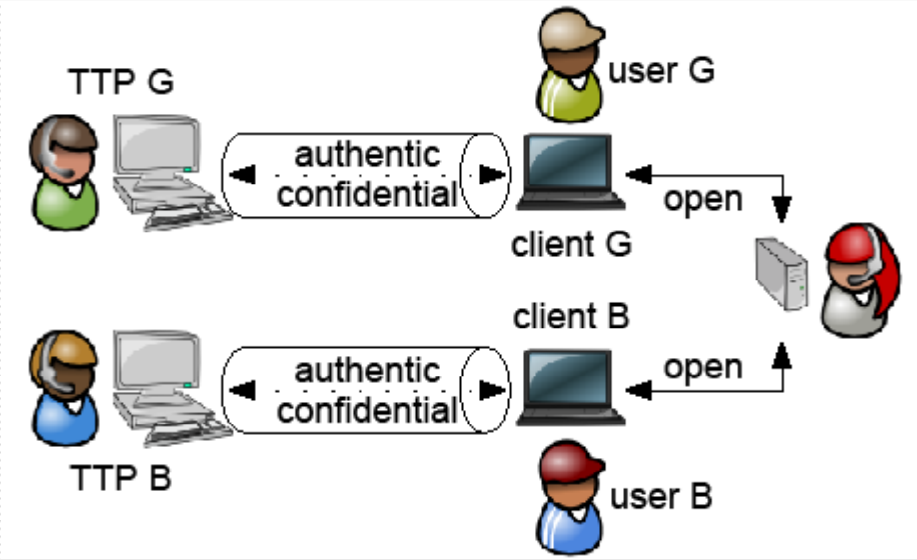
Requirements: Attackers



Protocol: Overview



Protocol: TPMs as TTPs



Protocol: Details

1			C	⟶	S	*REQ*
2			C	⟵	S	*PCR_INFO*, *N*
3	TPM	⟵	C			`TPM_CreateWrapKey`(H_P, *binding*, *non-migratable*, *PCR_INFO*)
4	TPM					assert K_P is *non-migratable*
						generate non-migratable binding key (K_C, K_C^{-1})
5	TPM	⟶	C			K_C, Enc_P(*binding*, *non-migratable*, *PCR_INFO*, K_C^{-1})
6	TPM	⟵	C			`TPM_LoadKey2`(K_C, Enc_P(*binding*, *non-migratable*, *PCR_INFO*, K_C^{-1}), H_P)
7	TPM	⟶	C			H_C
8	TPM	⟵	C			`TPM_CertifyKey`(H_C, H_{AIK}, *N*)
9	TPM	⟶	C			Sig_{AIK}(*binding*, *non-migratable*, *PCR_INFO*, *N*, K_C)
10			C	⟶	S	Sig_{AIK}(*binding*, *non-migratable*, *PCR_INFO*, *N*, K_C), Sig_{CA}(*aik*, K_{AIK})
11					S	assert K_{AIK} is *aik*
						assert K_C is *binding*
						assert K_C is sealed to *PCR_INFO*
12			C	⟵	S	$Enc_C(d_s)$
13	TPM	⟵	C			`TPM_UnBind`($Enc_C(d_s)$, H_C)
14	TPM					assert *C* is in state *PCR_INFO*
15	TPM	⟶	C			d_s

Security Analysis

- Informal analysis:
  - Secure against man-in-the-middle attacks given tamper-resistant RTs
  - Secure against dishonest users as well given tamper-proof RTs
- Formal analysis is highly desirable → opportunity for future work

Conclusion

- The protocol maintains the confidentiality of secrets in the face of eavesdroppers and careless users
- Given an ideal (tamper-proof) trusted platform, the protocol maintains the confidentiality of secrets even in the face of dishonest users