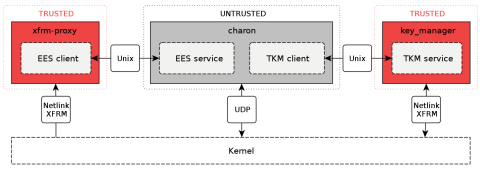
Adrian-Ken Rüegsegger

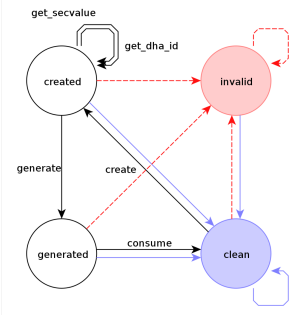
Graduate Candidate	Adrian-Ken Rüegsegger
Examiner	Prof. Dr. Andreas Steffen
Co-Examiner	Prof. Dr. Andreas Steffen
Subject Area	Software and Systems

IKEv2 Separation

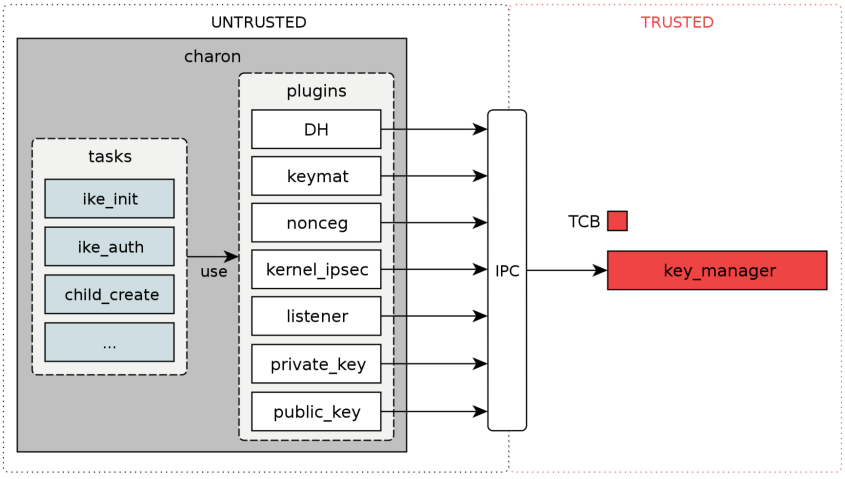
Extraction of security critical components into a Trusted Computing Base (TCB)



System overview



Diffie-Hellman context state machine



Split of IKE into trusted and untrusted parts

Introduction: The IPsec protocol relies on the correct operation of the IKE key exchange to meet its security goals. The implementation of the IKE protocol is a non-trivial task and results in a large and complex code base. This makes it hard to gain a high degree of confidence in the correct operation of the code.

Objective: We propose a component-based approach by disaggregating the IKE key management system into trusted and untrusted components to attain a higher level of security. By formulating desired security properties and identifying the critical components of the IKE protocol, a concept to split the key management system into an untrusted and trusted part is presented. The security-critical part represents a trusted computing base (TCB) and is termed «Trusted Key Manager» (TKM). Care was taken to only extract the functionality that is absolutely necessary to ensure the desired security properties. Thus, the presented interface between the untrusted IKE processing component and TKM allows for a small and robust implementation of the TCB. The splitting of the protocol guarantees that even if the untrusted side is completely subverted by an attacker, the trusted components uphold the proposed security goals.

Solution: The viability of the design has been validated through a prototypical implementation of the presented system. The untrusted parts of the IKE daemon have been implemented by extending the existing strongSwan IKE implementation. The trusted components have been implemented from scratch using the Ada programming language, which is well suited for the development of robust software. The new Design-by-Contract feature of Ada 2012 has been used for the implementation of state machines, to augment the confidence of operation according to the specification.