可信计算环境下的 IKEv2 协议扩展方案

肖跃雷 1,2,3，武君胜 1，朱志祥 2,3
(1 西北工业大学 计算机学院，陕西 西安 710072；2 陕西省信息化工程研究院，陕西 西安 710075；3 西安邮电大学 物联网与两化融合研究院，陕西 西安 710061)

摘要： 在 IKEv2 协议基础上，利用 ISO/IEC 9798-3:1998/Amd 1:2010 中的认证机制，提出了一种可信计算环境下的 IKEv2 协议扩展方案，实现了发起者和响应者之间的双向身份认证和平台认证，并建立了它们之间的会话密钥，且与 IKEv2 协议是向后兼容的，其中可信第三方（TTP）负责它们的身份证书验证、平台证明身份密钥（AIK）证书验证和平台完整性评估，它们的存储完整性度量日志（SML）被加密传输给可信第三方，从而有效地解决了现有可信计算环境下 IKE 协议扩展方案所存在的问题.此外，利用针对可信网络连接协议的串空间模型证明了该 IKEv2 协议扩展方案是安全的.

关键词： 可信计算；平台认证；串空间模型；IKEv2

Extended Internet Key Exchange Protocol Version 2in Trusted Computing Environment

XIAO Yue-lei 1,2,3, WU Jun-sheng1, ZHU Zhi-xiang2,3
(1 College of Computer Science and Engineering, Northwestern Polytechnical University, Xi′an 710072, China;2 Shaanxi Provincial Information Engineering Research Institute, Xi′ an 710075, China; 3 Institute of IOT and IT-based industrialization, Xi′ an University of Posts & Telecommunications, Xi′ an 710061, China)

Abstract： On the basis of the IKEv2, an extended IKEv2 in trusted computing environment based on ISO/IEC 9798-3:1998/Amd 1:2010 is proposed in this paper. It realizes mutual identity authentication and Platform-Authentication between an initiator and a responder, and establishes session keys between them, and is backward compatible with the IKEv2, where a trusted third party (TTP) is responsible for validating the identity and Attestation Identity Key (AIK) certificates of them, and evaluating the platform integrity of them, and the stored integrity measurement logs (SML) of them are encrypted and sent to the TTP. Thus, it is able to solve the problems of the existing extended IKE protocol for trusted computing environment effectively. Moreover, the extended IKEv2 is proved secure based on the strand space model for trusted network connect protocols.

Key words： trusted computing; platform-authentication; strand space model; IKEv2

作者简介：
肖跃雷男，（1979-），博士后，副教授.研究方向为可信计算、安全协议分析与设计、无线网络安全、大数据安全、数据分析与挖掘等.E-mail:xiao_yuelei@163.com.
武君胜男，（1962-），博士，教授.研究方向为计算方法、科学计算可视化、软件工程等.
朱志祥男，（1967-），博士，教授.研究方向为网络与信息安全、信息技术和信息化等.