计算机应用 2006 26 (09): 2116-2120 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

一种改进的Woo-Lam密码协议模型

赵宇[1]; 袁霖[2]; 王亚弟[2]; 韩继红[2,2]

解放军信息工程大学电子技术学院102教研室[1]

收稿日期 2006-3-29 修回日期 网络版发布日期 2006-8-31 接受日期

摘要 提出了一种改进的Woo-Lam密码协议模型，即eWoo-Lam模型。与Woo-Lam模型相比，新模型具有以下特点：增强了模型中关于密码学原语操作的描述语法，使得对密码协议主体行为的描述更加精确，提高了模型在检测协议攻击方面的能力； 引入了匹配运算机制，保障了模型安全性证明的有效性； 提出了七条形式化准则，规范了模型的抽象过程； 扩充了模型基于状态迁移的形式语义，使其更加精确合理； 重新给出了模型安全性的形式定义，使其更具一般性。

Abstract An improved Woo-Lam Model for cryptographic protocols, namely eWoo-Lam Model was introduced. Compared with Woo-Lam Model, the new model has such advanced properties as follows: to enhance the syntax of the model for cryptographic primitives, which enables the model to specify the principal actions more precisely and detect the attacks on the protocol more efficiently; to bring in match mechanism, which guarantees the effectiveness for the security analysis of the model; to propose seven formalization principles to normalize the procedure for model abstraction; to extend the state-transition based semantics to make it more rational; to redefine the security properties of the model to make them more generic.

关键词 密码协议模型 语法 形式化语义 安全特性

Key words Cryptographic Protocol Models;Syntax;Formal Semantics;Security Properties

分类号

DOI:

通讯作者:
赵宇 zhaoyn83@hotmail.com

作者个人主页: 赵宇 袁霖 王亚弟 韩继红