工程成果	复杂网络环境下服务安全提供方法及关键技术
申请人	李凤华
团队成员	李凤华、马建峰、李晖、李兴华、朱辉、耿魁
申请人自述	（请简述工程成果的目的和意义，解决了什么问题，有何贡献或影响，在何处应用，应用效果等。总字数不超过 1000 字，可附页） 该项目属于信息安全领域。包含互联网、移动网和物联网等具有开放性、异构性、移动性、动态性、多安全域等诸多特性的复杂网络系统已成为国家信息基础设施的重要组成部分，云计算、大数据等基于复杂网络的服务模式已广泛应用于国家重大行业，其安全是影响国家战略安全的主要因素，但目前缺乏系统化的解决方法。该项目结合国家战略需求，针对复杂网络下服务安全提供中的三个关键技术：数据服务安全、业务安全提供以及用户接入控制开展研究，发明了跨应用领域、可组合的专利群，形成了以下主要创新点： （1）提出了支持同名可信重构的 TPM 体系结构，解决了 TPM 内部信息的预置、备份与恢复、迁移等方面的安全问题，特别是 TPM 出现故障时，可实现其保护数据的迁移和恢复；设计了支持多算法并行、线程级随机交叉加解密方法，解决了多对多通信中多密码算法、多密钥、多数据流的随机交叉加解密问题，可高效支持多用户海量数据细粒度加密、多级安全保护和高并发数据处理。 （2）提出了基于模式匹配的网络业务流识别方法，满足大规模在线高并发业务请求的预处理需求；提出了支持高并发的业务数据处理技术，采用应用服务器与后台业务处理模块多级联动的全流水方式，解决了百亿量级在线并发业务处理问题，为大数据中心的海量用户和瞬时海量业务处理提供强有力的技术支持。 （3）提出了适用于复杂网络环境的动态接入认证方案和信任评估方法，解决了多域用户间信任评估和动态群组用户安全接入与信息共享的问题，可有效支持海量用户信息的安全动态共享与

	分发；设计了基于多要素的访问控制方法，可有效支持复杂网络环境下“浏览器—应用服务器—数据库服务器”的细粒度动态访问控制。 由方滨兴院士为组长的鉴定委员会一致认为“该项目研究难度大，取得成果丰富，其成果系统性强，总体处于国际先进水平。其中，支持同名重构的 TPM 体系结构、支持百亿量级的在线并发业务数据处理方法、支持多算法/多密钥/多数据流随机交叉加解密方法等关键技术处于国际领先水平”。获 2014 年度中国通信学会科学技术奖（技术发明类）一等奖。 项目成果符合国家信息安全战略发展部署，为国家在云计算、金融和数据库等不同领域安全、自主、可控的信息安全战略提供了坚实的技术支撑。