| | |
|---|---|
| 工程成果 | 智能终端可信运行环境构建关键技术研究 |
| 申请人 | 于爱民 |
| 团队成员 | 于爱民，汪丹，张妍，晏敏，杨文思，敖赢戈，周启惠，杨溢学 |
| 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）<br>随着移动互联网的快速发展，智能移动终端越来越多的参与处理涉及隐私、财产、商业或技术秘密的数据信息，因此成为众多攻击者感兴趣的攻击对象，安全攻击事件频繁发生，严重阻碍了智能移动终端的发展。为此，解决智能移动终端的安全问题迫在眉睫。为构建可信的智能终端运行环境，我们从智能移动终端安全体系架构出发，对智能终端完整性度量技术、权限技术进行了研究，并取得了一定的研究成果。其中，我们提出的新型智能移动终端安全技术体系架已被广电TVOS工作组初步接纳作为参考架构，研发的完整性度量系统实现了基于地理位置对运行终端的完整性保护，研制的权限管理系统可以有效抵御权限提升攻击实现对运行系统资源的保护。<br>针对智能终端安全体系架构，我们从硬件层、内核层、系统服务层和应用层四个方面全面考虑智能移动终端的安全保障措施，构筑安全防护体系，提出了新型智能移动终端安全技术体系架构。并基于该体系架构，针对广电 TVOS 智能电视操作系统提出了 TVOS 系统安全体系架构，已被 TVOS 工作组初步接纳作为参考架构。<br>在完整性度量技术研究方面，我们基于可信计算构建可信终端的机理，首先研究构建适用于智能移动终端的信任根，研发了安全芯片仿真系统，然后基于该仿真系统作为信任根来研究度量终端完整性，研发了完整性度量系统，实现了对 Android 系统内核模块、Dalvik 虚拟机等的完整性保护，同时还引入了地理位置因素来控制终端完整性，基于地理位置监测终端是否位于敏感区 |

| | |
|---|---|
| | 域来决定对完整性不符合要求的应用的处理。<br>在权限技术研究方面，我们针对 Android 权限机制易遭受权限提升攻击的问题，对 Android 权限机制进行了全面解剖分析，研发了基于调用链的权限管理系统，通过为访问系统资源的应用组件构建调用链，并针对调用链制定资源访问策略，保证只有整个调用链的权限满足要求才能访问系统资源，避免了恶意无权限应用通过调用有权限应用来提升自身权限获取资源，有效保护了运行系统资源的安全。<br>基于上述研究成果，我们已撰写了多篇科研论文并分别投稿国内外期刊和会议，目前已发表 1 篇，还有 1 篇译著即将出版。同时，我们已提交 1 项专利申请，获得了 2 项软件著作权授权。 |