《学科前沿讲座》学期报告

**班号： 232115 学号： 23373125 姓名： 付宁远**

|  |  |
| --- | --- |
| **学术报告参与情况**  （建议每学期两次及以上，大二大三总计参与8次讲座，不封顶，可加行） | |
| **报告时间** | **报告主题** |
| 5.28 | 安全操作系统设计方法简介 |
|  |  |
|  |  |
|  |  |
| 学习总结：围绕某期报告或多期报告，总结所学所感，鼓励有自学、有拓展，字数不少于500字。  黄辰林博士作为国防科技大学计算机学院研究员、国家科技进步一等奖获得者，在操作系统安全领域拥有深厚的理论造诣与丰富的工程实践经验。其报告以“安全操作系统”为核心，系统梳理了其发展脉络，并前瞻性地指出智能与泛在计算时代下的新挑战，令人深受启发。  报告的核心价值在于清晰地勾勒出安全操作系统的演进图景。黄博士并非停留于抽象理论，而是结合其主导研制的银河麒麟操作系统安全可信子系统、麒麟铠衣高可信系统等国家级重大工程实践，生动展现了安全理念如何在技术迭代中具象化：从早期主要依靠隔离与访问控制机制构建基础防护，到网络时代引入形式化验证、增强型访问控制模型（如BLP、Biba） 以应对更复杂威胁，再到当前云环境与万物互联背景下可信计算基（TCB）最小化、基于硬件的可信执行环境（TEE）、机密计算等成为关键。这种依托于实践的演进分析，使得抽象的安全设计理念变得具体可感。  尤为深刻的是，报告精准揭示了当前智能计算与泛在计算场景为操作系统安全带来的颠覆性挑战。一方面，智能应用的动态性、数据驱动特性使得传统静态安全边界模糊，模型安全、训练数据隐私、对抗样本攻击等成为操作系统必须协同防御的新维度。另一方面，泛在计算中海量异构、资源受限的终端设备接入，极大扩展了攻击面，对操作系统的轻量化安全架构、细粒度动态信任管理、设备身份可靠认证提出了前所未有的高要求。黄博士指出，未来研究必须致力于解决这些矛盾：如何在保障高性能与低开销的同时，实现跨智能模型、泛在设备的内生安全与动态信任链构建？  黄博士的报告不仅是一次知识的梳理，更是一场思想的动员。它深刻阐明：操作系统作为数字世界的基石，其安全性已从单纯的技术问题上升为关乎国家信息基础设施命脉的战略要务。在人工智能与物联网浪潮席卷全球的今天，唯有持续推动操作系统安全技术的自主创新与前瞻布局，方能在复杂严峻的网络安全态势中筑牢根基，护航数字中国的行稳致远。报告所点明的方向——融合智能特性的内生安全、面向泛在环境的动态可信——无疑是未来攻关的核心命题，对学术界与产业界均具有重要引领意义。 | |
|  | |
| **学习照片：**一张听报告照片/截图，本学期为课改试行学期，如无照片可不粘贴。从下学期起，需提供至少一张学习照片。 | |