能够容忍入侵并在线恢复的数据库安全新技术研究

立项依据：项目意义

关系国计民生的军队、政府、通讯、电力、金融、交通等领域：

- 信息系统后端都有一个（或更多）数据库作为支撑
- 重要的大型数据库不断增加 → 攻击行为也在迅速增加
- Microsoft、Oracle、IBM公司的产品暴露出65个安全漏洞
- 信用卡、银行、空中交通管制、物流管理、库存追踪、网上股票交易、电子商务等数据密集型应用的攻击案例
- 互联网上爆发的大规模的 SQL Slammer 和 SQL Snake 攻击

说明：多种攻击方法确实能突破数据库保护机制，严重地威胁经济、社会和日常生活

由于无法完全阻止，能够容忍一定程度的攻击行为的数据库安全技术是一个非常紧迫的研究课题。

立项依据：项目意义

国防领域、信息化战争背景下：

- 1991年的海湾战争、1999年的科索沃战争、2003年的伊拉克战争
  - 表面：获取情报快、指挥决策活、打击目标准
  - 实质：指挥决策、作战计划和武器控制依靠的则是其强大的军用数据库系统
  - 说明：数据库是信息化战争中的一个核心、战略资源
- 传统领域的数据库技术
  - 依赖：访问控制、各种完整性控制、值域约束、并发控制和恢复、自动复制
  - 目标：提高数据的可靠性、可用性
- 在信息战下，传统措施有效性不够，导致数据泄露或破坏，造成“数据污染”
  - 在信息战下，正常的访问控制可以被攻破
  - 内部的授权用户可能由于贪婪、心情沮丧等原因被利用而成为攻击者
  - 攻击者可能通过各种方式取得合法用户身份，获得相应授权

  更糟的是，传统技术中用于维持数据之间一致性的措施反而把“污染范围” 扩大

因此：国防领域的基本假设是：并非所有的攻击都能够被成功阻止。

提高数据库的抗毁性和动态恢复能力，保证受到敌人攻击后，能继续工作并能从被攻击的状态中恢复，是支撑信息化军队展开作战行动并赢取胜利的关键技术。

项目目标—威胁模型

针对军队、政府、金融、通讯等关键领域、价值巨大的数据库的攻击模式：

- 不一定体现在彻底击毁数据库，使之不能对外提供服务上。因为这种攻击行为的隐蔽性不够，会被立即察觉，从而丧失长期或进一步操控系统的机会。
- 相反，更多的攻击行为倾向于
  - 窜改数据库中的数据来牟取利益，如窜改金融数据库中的帐户余额
  - 误导基于这些数据的决策，如信息化战争中对剩余军力和各种技战术指标的修改

本项目提出的数据库安全新技术专门针对这种潜伏性强、危害大、对抗难度大的逻辑攻击，它假设攻击者通过发起恶意的事务来破坏数据的准确性、一致性和完整性

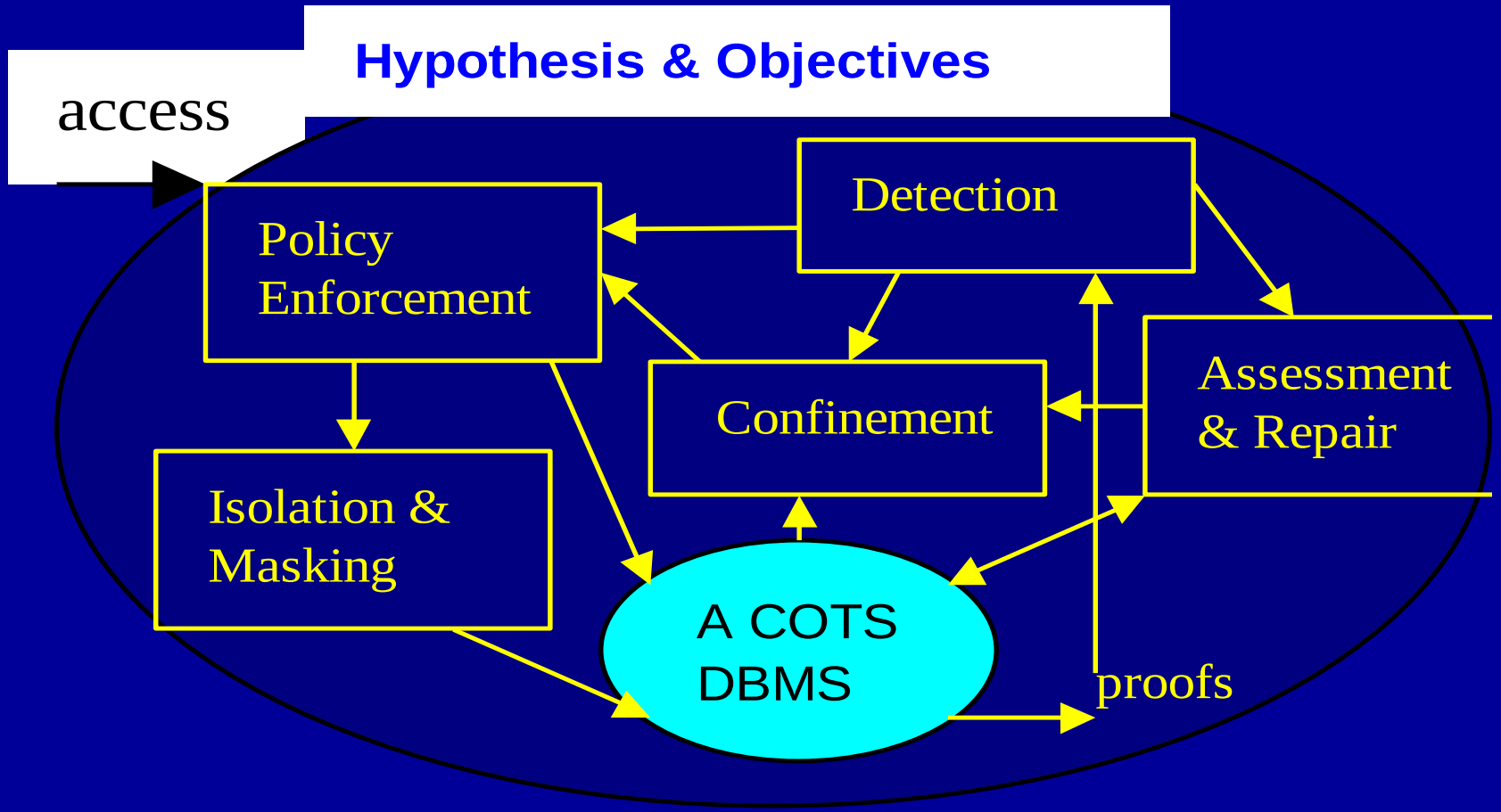
项目目标

- 提供全面、高效、基于商品DBMS的数据库容忍攻击和动态恢复的核心技术
- 当遭受到攻击时，这些技术能帮助数据库系统根据受到攻击的情况自行调整应对措施和系统配置，保存核心运行能力，并逐渐修复数据
- 修复数据的同时，数据库保持在线服务状态，用户还能利用系统保存下来的能力来处理事务
- 并且保证一定程度的（根据用户定义的安全策略）数据完整性

创新点

- 能够容忍一定程度的入侵行为
- 动态、在线修复入侵行为造成的数据损伤
- 针对商品DBMS，不修改DBMS代码

技术路线－1



An intrusion tolerant DBMS

技术路线—2

- 基于已有DBMS商品的多层次的主动式防御框架，层次之间能够相互协调，动态配合
- 基于语义特征的数据库事务级的入侵检测技术
- 基于用户级别的、优化的、高效的入侵隔离技术
- 多阶段的损伤定位和限界技术；动态的、在线的损伤评估和修复技术

试验方法

- 在一个现有的商品DBMS上开发一个试验系统来验证对入侵的容忍能力，系统中各部件采用CORBA框架协同
- 进行事务级别的入侵检测试验，评估事务语义在入侵检测中的有效性
- 进行事务隔离、用户隔离试验，评估新技术的效率
- 进行损伤限界试验，评估多阶段的限界技术的有效性
- 进行损伤评估和修复试验，评估修复时间对数据完整性产生的影响。
- 对整个系统进行集成试验，评估整体的成本效益和性能