**个人信息**

|  |  |  |
| --- | --- | --- |
| **姓名**：**沈坤** | **手机**：182 1371 8616 (微信同号) | **邮箱**：[shenkun@bupt.cn](mailto:shenkun@bupt.cn) |
| **意向**：数据库/安全/后端 | **城市**：成都、北京、其他 | **年龄：**26 (1998.10) |

**教育经历**

|  |  |
| --- | --- |
| **北京邮电大学 网络空间安全学院 (原属计算机学院) 信息安全专业 本科 2016.09 - 2020.07** | |
| **计算机课程** | 操作系统、计算机网络、数据库系统、数据结构、C语言程序设计、计算机体系结构等 |
| **安全课程** | 现代密码学、网络安全、系统安全、软件安全等 |

**工作经历 (4.3年)**

|  |
| --- |
| **华为 2012实验室--高斯实验室 数据库内核开发 高级工程师(16级) 2020.07 - 至今** |
| **职责** 分布式OLTP数据库**GaussDB**、开源数据库**openGauss**中，作为多特性的独立或核心开发者，9版本累计设计交付**10个需求**，提交**1w+行核心代码**，其中7个需求已商用；作为安全接口人,分发1000+产品问题  **能力** 熟悉GaussDB全部的**11个关键安全特性**：1)开发：透明加密、密态等值查询、机密计算；2)维护：安全传输、加密函数；3）熟悉：身份认证、访问控制、安全审计、数据发现、数据防篡改、数据脱敏  **其他** 熟悉PostgreSQL与GaussDB执行、存储、驱动等**10+子模块**的设计、源码、调试等 |

**项目经历**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **1 华为 GaussDB表级透明加密特性 工商银行即将商用 2022.12 - 2024.09**   |  |  | | --- | --- | | **原理** | 在存储模块，落盘数据时，自动加密数据，读取数据时，自动解密数据，自动管理密钥，实现存储安全 | | **功能** | 1)加密对象：9种表、2种索引；2)加密范围：堆表文件、redo-log、undo-log、双写数据；3)间接加密范围：主备复制流、物理备份集等；4)加密管理：采用3级加密模型，对接3种密钥服务，实现表级密钥独立，支持多种5加密算法，支持密钥轮转；5)安全合规：基于GMT-0018接口对接第三方加密机 | | **性能** | 实现6个高性能设计，TPCC测试中，加密全部表、索引、redo、undo日志，主备场景性能劣化在1%内 | |
| **2 华为 GaussDB密态数据库特性 华为ERP系统已商用 2020.07 - 2022.11** |
| |  |  | | --- | --- | | **原理** | 在数据库驱动，以列为粒度，自动加密SQL中的数据，自动解密查询结果中的数据，自动管理密钥；在执行模块中，基于机密计算框架，解决密文安全运算；实现数据传输、计算、存储安全 | | **功能** | 支持在密文上进行等值查询、范围查询、模糊查询、内置函数计算、排序等操作，采用3级加密模型，对接3种密钥服务，基于机密计算框架，在数据库内存无明文的约束下，实现常见DML操作 | | **性能** | 实现4个高性能设计，在TPCC测试中，加密1个表，性能劣化在30%内，高于同场景Azure的50%劣化 | |
| **3 个人 独立OLAP数据库小项目kkdb https://gitee.com/lorand/kkdb 2023.09 - 2024.05** |
| **功能** 支持简单DDL与DML语法，实现语法解析、语义分析、缓存区、事务、数据组织等多模块，支持高并发 |
| **4 北邮 基于netfilter的包过滤防火墙 2019.11 - 2019.12** |
| **功能** 在Linux网络栈，基于Netfilter框架，实现4种静态、2种动态的包过滤功能，支持检测与预防1种欺骗、3+3+5种信息采集、6种DOS攻击 |
| **5 北邮 基于国密的全加密网盘 2018.09 - 2018.10** |
| **功能** 实现非标国密SSL，支持数据加密传输；实现国密口令身份认证；支持国密加密存储文件数据与元信息；支持线程池；支持GUI客户端 |

**能力范围**

|  |  |
| --- | --- |
| **操作系统** | 熟悉CPU原理、内存管理、进程线程管理、文件管理、设备管理；熟悉linux编程 |
| **计算机网络** | 熟悉应用层、传输层、网络层、链路层等协议原理；熟悉socket编程 |
| **编程能力** | 熟悉C、Python语言；熟悉常见数据结构、算法；了解汇编原理、编译原理;Leetcode 400+题 |
| **密码学** | 熟悉常见对称、非对称、哈希算法原理与应用；熟悉密钥全生命周期管理；熟悉PKI体系 |
| **网络安全** | 熟悉网络欺骗、信息搜集、拒绝服务等攻击原理，熟悉SSL等协议、熟悉防火墙等机制与实现 |

**实习经历**

|  |
| --- |
| **经纬恒润 整车安全部 信息安全实习生 2019.02 - 2019.08** |
| **职责** 分析标准ISO-15408(即CC)、AUTOSAR-J3061，分析车联网攻击事件，爬取全国300+市20年天气数据 |

**技能爱好**

|  |  |
| --- | --- |
| **博客** | 习惯总结学习笔记，华为内网上传70+篇博客，累计帮助20+部门同事，20+一线 |
| **工具** | 日常使用git、gcc、gdb、perf、benchmarksql、curl、openss等工具 |
| **书籍** | 对照postgresql源码，阅读多本postgresql内核解析书籍 |
| **其他** | 良好的英语阅读能力，一般的口语能力，四级525。较好的文档撰写与PPT制作能力 |