**王浩** **软件设计与开发（C++）**

河南省巩义市 Tel: 13501764824 E-mail: [atlantiswang@foxmail.com](mailto:atlantiswang@foxmail.com)

addr: <https://github.com/atlantiswang> <https://blog.csdn.net/wh_2396>

教育经历：

2010.10 - 2014.6 河南农业大学 电子信息科学与技术专业 本科

**培训经历**：2014.8 - 2015.3

在校学习的内容偏向理论，不太符合企业需要，就通过培训快速提升一下适应企业的能力。

主要内容为：

C/C++ 基础 STL数据结构与算法

Unix/linux C/C++ Win C/C++ MFC Qt COM组件

数据库（ORACLE）Socket

所做项目：

培训结束后去了一家与培训机构合作的公司做了一些工作 2015.3 - 2015.6

Dms数据挖掘

根据需求编写文档、代码

c/s架构的系统。client端搜集整理登录的信息，通过socket发送到server端。server端放入数据库

wtmpx文件存放的是登录的主机ip等信息。client通过读取wtmpx文件的信息，通过logout记录提取出登录的信息，通过socket发送到远程server端。

Server端有一个生产者-消费者模型的buff类。生产者线程将通过socket接收到的登录信息push进buff，消费者线程将buff中的信息一条条提取出来存入数据库（oracle）。

windows数据挖掘系统：

同上一个系统的整体功能类似。但平台是windows，更加复杂一些，而且是分三个模块：

exe：搜索数据（通过winhttp）从航空公司官网抓取数据并放入mysql数据库database1。此终端专门负责抓取数据，而且是一轮一轮快速地抓取，以保证数据库的数据与网站同步。

Client：从database1中查询数据并处理数据，发送给server。

Server: 从Client接收数据并通过携程接口上传携程官网，使用MFC AsyncSocket。

**工作经验**

**上海格尔软件股份有限公司** 2015.7 - 2016.3 100 - 499人 A股上市 ￥7000

第一份工作，时间不长，公司主要做数字安全产品，工资不高但办公环境干净，能培养新人,代码管理规范。定期技术分享与竞赛。工作中需要了解并使用各种加密算法。

技术点：SM1\SM2\SM3\SM4\hash\DES\RSA 数字信封、数字签名、PKI、PKCS（公钥密码学标准）、MFC、win32、duilib

工作内容：

网盾PC保护维护：

需要了解windows的登录原理（xp用gina，xp以上用credentialprovider）

网盾保险箱维护

所做项目：证书助手工具的开发

证书助手是用来管理PC端的usbkey的。与PKI服务端的RA交互来完成对证书过期的提醒、延期申请、密钥更新、密钥恢复、用户信息修改的申请与操作。 客户端的数据请求通过post请求来完成(winhttp)。并对服务端返回的信息进行解析。数据模式采用json.界面前期使用MFC。后期改为duilib。

**北京中软华泰信息技术有限公司** 2016.4 - 2019.5 100人 ￥10000-16000

北信源收购 内网服务器终端安全 主要产品：操作系统加固、 EDR检测

采用c/s架构。client为安装在内网服务器上的终端软件（所以在这里内网的服务器被看作客户端），server为一台Java开发的机器，与各个client。提供注册、下发策略，显示审计等控制功能。并提供b/s的web页面给管理员使用。

\*操作系统加固：

工作内容：维护为主开发新功能为辅、工作比较杂碎。现已经封版

技术点： C++、stl、进程间通信、线程同步、sqlite数据库、socket、内核驱动、 qt\MFC、session隔离、调试（远程调试、windbg、ida）、远程线程注入

产品形态：服务进程+QT界面进程+内核。

服务进程负责与管理中心通信。

内核有文件过滤驱动、注册表过滤驱动。

熟悉的功能：

白名单 白名单分组上传 进程防杀 网站防护（asp，httpmodule） 可信连接

\*EDR终端检测与响应

工作内容：构造整个项目的骨架、部分检测模块的编码与维护。开发中。

技术点：socket、生产者-消费者模式（windows下采用信号量与互斥实现），开源库编译

主程序为一个服务程序，并配有一个托盘程序，实现注册\重注册功能。

生产者消费者模型使用一个单独的类提供缓冲区，并提供product、consume方法调用。

服务程序创建生产者线程、消费者线程（1个）；

生产者线程的实现在各个dll中，不同的dll采集不同的检测内容。有多少个dll就有多少个生产者线程。服务程序调用各个dll的时候，将缓冲区类实例的地址做为实参，缓冲区类对象的抽象类指针做为形参，从而接口与实现分离。

各个检测dll：

进程管理、服务管理、网络管理、资产管理、账户管理

弱口令检测、合规配置检测、网站安全检测（webshell）、主机漏洞检测

使用的开源库：

Mimiktatz

Ovaldi

yara

libevent

**总结**：