# 安全架构

## ****内容介绍****

本篇是系列文章的第十一篇，分享一下自己对安全架构的看法。安全架构用于指导安全建设，不同架构师的架构是不一样的。

本系列文章仅表示本人的架构思想。

如有雷同，纯属巧合。如有不同，纯属正常。

## 架构的理解

我国最知名的架构是阿里的中台架构，后来阿里将中台又进行了架构设计，拆出了更多的中台。

伴随着企业发展，量变会引起质变。企业工作及问题的复杂度会爆炸性增长。单以软件开发举例，十几个用户的时候，不会对性能，数据库，语言等有所要求。使用单线程的python，使用文本文件当数据库，都是可以的。但是要服务几百万，上亿的用户的话，那么会出现方方面面的各种要求，从物理IT设施到网络，到协议，到语言，到软件，一整个链路都是需要考虑的。

为了解决复杂度问题，于是架构出现了。

架构是伴随着复杂度而出现的，复杂度有限的工作，没有架构出现的土壤。

公知有一个说法，说世界语言，只有汉语停止进化了，几十年几百年没有变化。其他语言，如英语，一直在进化，一直有新的词语出现。

对此，我的看法是，汉语的架构师非常牛逼，英语的架构师非常傻逼。所以英语应对不了复杂度，每出现新事物都必须造一个单词。最长的英语单词是肺尘病，有45个母。有非常高的维护成本与学习成本。

架构也有大小，阿里的中台是公司级的架构，涉及技术，组织，管理等共同组成，小的架构有某软件某模块某功能的抽象。

## 架构师的理解

架构是一种思想，不是一个职位。董事长，总裁，总经理，架构师，小组长，员工都有架构的思想跟能力，区别只是面向的对象不同。董事长的对象是整个公司，总裁的对象是对应的职责模块，总经理的对象是对应的业务，架构师的对象是某系统，小组长的对象是某模块，员工的对象是某功能。

架构师工作，做的是架构建设以及架构升级。

差的架构，可能只能服务公司一年。好的架构，可以服务公司五年。

但是随着企业的发展，架构终会迎来自己的能力极限。这时候就需要对架构进行升级，搭建新的架构。

比如说阿里公司层面，从无中台，到单中台到多中台。涉及到技术、管理、组织、运营等方方面面，影响到每个人。而系统的重构，也是架构升级，只会影响到开发。

架构，是伴随着复杂度而出现的，是为了解决现实问题而出现的，是跟业务紧密相关的。比如中台架构适合阿里，但是不一定适合其他公司，因为业务都不一样。

比如互联网行业与汽车行业。主要产品就不一样，一个是APP，一个是汽车。

汽车极度看重安全设计，因为物理架构影响软件架构，软件影响功能。如果设计阶段安全没搞好，最后车辆卖出去了，但是又发现了安全问题，那就只能召回修复。

但是APP的设计安全就不是那么重要，因为可以强制升级，升级很快。特别是微服务架构，Devops模式，把修复成本都拉平了。

即便是同样的电商业务，阿里多中台了，其他公司可能不需要中台。

架构里，在一个阶段可以打包的事情，到了公司另一个阶段，可能要把它拆开再细化。

体现在招人上，就是越来越要求匹配度，越来越要求专业度。

## 如何进行安全架构

公司战略服务于国家战略，比如华为坚决不造车，造车的生态位有比亚迪有新势力了。比如蚂蚁被叫停上市，杠杆太大了，容易引发系统性金融风险。

安全战略应服务于公司战略。比如阿里的使命是让天下没有难做的生意，它的战略是搞电商平台。

如果我是阿里安全负责人的话，那么安全的目标就是让人们在平台上放心的做生意。

实现这个目标的战略是 搭建信任的交易体系，搭建风控体系，搭建信息安全体系，搭建网络安全体系。

架构师的核心能力是如何从企业目标，构建出自己的安全目标，拆解出来安全战略，再到安全战术。具体的战术实施，应由团队实现。架构的好坏，看的是性价比。即成本与支持的时间。照着大公司的架构抄很容易，但是成本能接受吗？开发只有20个人，但是安全架构落地要30个人，这个架构有什么用？

安全服务于公司，安全战略及安全架构要支撑公司总体战略。

架构是从上往下的规划，是分层的。安全负责人，负责总架构，安全方面负责人，负责安全方面的架构，支撑总架构。

架构落地实现，是从下往上的，逐步给上面实现支撑。

功能安全设计、评审、验证测试等，为业务安全、应用安全提供支撑。

DLP设备、信息分类分级等，为信息安全提供支撑。

HIDS、流量监测设备等，为基础IT设施安全提供支撑。

以上为整体安全提供支撑，整体安全为企业安全提供支撑。

拆分通用性安全，与特殊安全

下级安全架构，发现潜在通用安全。

架构是中间层，往上对接目标，往下对接实现。

是一个拆解的过程。

安全平台：方法论，案例，工具，技术，系统，体系，流程，规范，标准等等组合而成的平台。

架构，受制于公司。

所以能进大公司最好进大公司

公司内安全的战略位置，可以看安全负责人的汇报关系，像CEO汇报，还是CTO，还是技术总监，还是当一个挂件。

不要裸辞，裸辞没法保证，下个公司平台比上家更好。

业务的IT相关性越高越好，互联网就跟IT强相关，医疗就跟IT相关不大

如果能搞到安全负责人的履历资料，看负责人的履历也行。

好处是能力培养与引导，引导很重要，公司层面的就是职级成长体系，工作层面的就是领导的专业性。

什么是优秀的公司？

所有公司存活都是基于需求的，市场的大小，限定了公司规模。

基于需求的公司，非常依赖创始人。

基于需求的公司，应该尽快转型成为基于架构的公司。

基于架构的公司，更能捕捉新需求。

运维架构以及开发架构都在进步

运维由传统物理机，到虚拟化， 到云，到docker

基础IT设施安全架构也推陈出新，提出了云安全，提出了容器安全。

开发架构由传统，到敏捷，到devops

应用安全架构也由SDL发展到了devsecops

互联网跟软件，对非互联网业务的影响

总体安全架构也应该随之进化调整。将通用部分跟与业务紧密耦合的部分区分出来，抽象出来。

公司战略，业务战略，特别是大公司，复杂度极高。有必要建设一套平台来支持工作，形成可复用的能力，极快的成长。否则按照每个业务去进行安全支持建设，会非常没有性价比。

成熟优秀的，行业领先的架构，是迭代而来的。点柴火是不需要架构的，但是点火箭，就需要。

公司有通用安全方面，比如基础IT设施安全，应用安全，办公安全。

也有跟业务强相关的安全方面，比如造车的，车里面ECU安全，软硬件，底层系统都有。比如云厂商，云本身的安全性。比如游戏，反外挂反灰产。

根据业务情况分，从软件到嵌入式到硬件，其安全要求就有很大区别。

APP完全不需要考虑安全系统的情况，不需要考虑链接WIFI用什么协议，怎么实现，有什么安全问题。

但是操作系统厂商，就需要考虑这些。嵌入式就需要考虑，系统要支持各种格式类型的WiFi链接，支持蓝牙链接。但是系统，不需要考虑，物理硬件被人刷写怎么办，替换怎么办？

安全硬件，如苹果手机里，有些模块是不能替换复用的。它的几个硬件之间，是有硬件的信任链的。要换只能都换。比如有的硬件falsh设计为只能刷写一次，重复刷写根本写不进去。

抽象思考，把能复用的东西抽象出来，做成安全基础服务，对其他部门提供。

假设我是华为的安全负责人。华为复杂性，有硬件，嵌入式设备，有操作系统，有软件，有云。有汽车，手机，通信基础设施，还有纯研究性质的专利，工业基础软件。

总部有一个安全团队，提供全华为的基础设施安全。每个行业设一个负责人，负责手机，负责云，他们对总部提需求，总部负责建设共用的基础能力。

## 中台的出现

组织中台，任务中台

人力分配

中台面临复杂度，通用工具。

## 抽象原则

### 组织及管理

组织及团队设置。

工作流程

规章制度

从项目/产品源头进行安全介入，与产品经理一同进行设计工作，在原始设计基础上添加安全需求进行安全设计，输出给开发团队。

代码开发规范，代码审计设置规则。

### 技术

通用安全技术

### 运营

安全事务的运营。建设过程推进也是运营，安全PMo。

## 安全方面划分

应用安全

基础安全

办公安全

数据安全

等多个安全方面

硬件安全

嵌入式安全

操作系统安全

技术栈以及技术链路

持久化，自动化，数据化，智能化

人才梯队体系

持久化可替换体系

安全岗位，与其他部门岗位有所不同。

假设这样一种情况，整体公司正常发展，各部门都有

其他单独能展开工作，没有这个角色，这件事就没法做，做不了。

但是没有安全，企业安全是有可能做的。

安全内生，安全培训很重要，安全意识的培养很重要。不能只搞运动式的进行安全意识培养，应该将安全潜移默化的植入到工作流程中。从入职的第一步，签合同就有在提信息安全，后续的新员工，日常工作中，在体系，流程，技术能力，文档等等所及的地方，都有信息安全的内容，是最好的培养信息安全意识的环境。

攻防，两个方向不一样。绩效评定之前，找乙方服务打一次，以结果评定工作效果。

## 通用安全

### ****安全培训****

应用安全的保护对象是应用系统，应用系统有各种表现形式，如Web、APP、小程序、客户端、系统等。应用安全就是围绕着这些应用的安全建设工作。

## 安全合规

安全培训

攻防对抗

安全情报

SRC

付费情报

乙方

资产梳理及管理

组织与制度建设

安全监控及发现

安全分析与评估

安全检查与测试

安全修复与处置

安全加固与防护

安全审计与报警

持续运营与优化