

## 02 | 安全原则：我们应该如何上手解决安全问题？

2019-12-09 何为舟

安全攻防技能30讲

[进入课程 >](#)



讲述：何为舟

时长 17:30 大小 16.03M



你好，我是何为舟。

上一讲，我们一起拆解学习了 CIA 三元组，也就是机密性、完整性和可用性。它们分别代表了数据的“不可见”“不可改”和“可读”。简单来说，以购买极客时间专栏为例，机密性就是未付费用户无法学习这个专栏，完整性就是这个专栏的内容不会变成别的其他方向的内容，可用性就是你作为付费用户，能够随时学习这个专栏。

理解了 CIA，上一节最后面试官问的“安全是什么”的问题，你现在一定可以回答出来了。面试官点点头，接着说道：“你觉得该怎么去解决安全问题呢？”

毫无疑问，不同的应用、不同的模块会受到不同的安全威胁，当然，我们面对这些威胁也会有不同的解决方案。万变不离其宗。正如安全威胁都是针对 CIA 三元组产生的攻击一样，安全解决方案在根本思路上也都是相通的。

今天，我就从方法原则这个层面上，来给你讲讲安全解决方案的主要思路。这块内容看起来比较偏理论，我尽量多从实践角度来给你讲我的理解，但是你一定要耐心看完，这样可以确保你对后面实践的内容能够理解得更加深入。

## 什么是“黄金法则”？

对于安全解决方案来说，不同的教材会有不同的解释。就我个人而言，我比较喜欢“黄金法则”这种理解方式。下面我就用这种方式来具体给你讲讲。

黄金法则主要包含三部分：认证（Authentication）、授权（Authorization）、审计（Audit）。为什么称它为“黄金”呢？一方面是因为，它包含的这三部分重要且通用；另一方面是因为，这三个单词的前两个字母都是 Au，而 Au 在元素周期表中代表着“金”。

有的教材中，会给黄金法则加上问责（Accounting）这一部分，组成“4A 法则”；还有的会加上身份识别（Identification），组成“IAAAA 法则”。不管被划分为几个部分，这些法则的中心内容都是相似的，都是围绕着**识别、认证、授权、审计、问责**这五个部分展开的。因此，黄金法则其实就是 IAAAA 法则更高一层的概括，它将识别和认证、审计和问责归纳到了一起，更加强调了这两两之间的协同性质。

搞清楚了“黄金法则”的概念，我们现在来看它的三个部分（认证、授权、审计）。这三部分其实是一种串联的关系，它描述的其实是用户在使用应用过程中的生命周期：**先进行登录、再进行操作、最后留下记录。**

## 认证

你是谁？确保身份的可用性

## 授权

通过你能做什么？确保行为的可信

## 审计

你做了什么？再次核验身份和行为的可信性



下面，我们就——来看这三个部分。

### 1. 身份识别和认证

首先，我们先来了解一下黄金法则的第一个部分：认证。认证其实包括两个部分：身份识别和认证。身份识别其实就是在问“你是谁”，你会回答“你是你”。身份认证则会问“你是你吗”，那你要证明“你是你”这个回答是合法的。

身份识别和认证通常是同时出现的一个过程。身份识别强调的是主体如何声明自己的身份，而身份认证强调的是，主体如何证明自己所声明的身份是合法的。比如说，当你在使用用户名和密码登录的过程中，用户名起到身份识别的作用，而密码起到身份认证的作用；当你用指纹、人脸或者门卡等进行登入的过程中，这些过程其实同时包含了身份识别和认证。

通常来说，不管你以什么形式进行登入，在身份识别的过程中，这些形式最终都需要落地成唯一的身份 id。在你后续的操作中，身份 id 都会始终跟随会话，记录在日志中。这也是后续授权、审计和问责的基础。身份识别的过程并不关注合法性，因此，认证是这个部分中最为关键的一环。

依据具体的认证场景，对安全等级、易用性等的综合考量，认证形式可以大致分为三种。按照认证强度由弱到强排序，分别是：

你知道什么（密码、密保问题等）；

你拥有什么（门禁卡、安全令牌等）；

你是什么（生物特征，指纹、人脸、虹膜等）。

我们通过将多种类型的认证进行组合，可以形成多因素认证机制，进一步加强认证强度。常见的，在登录过程中，很多应用会在输入完账号密码后，让你进行手机验证，这其实就是结合了“你知道什么”和“你拥有什么”的双因素认证。

**可信的身份认证是建立安全保障体系的第一步。**如果身份认证被破解，则后续的保护或者补救机制都无法起到太多的效果。因此，很多时候，通过衡量一个应用的认证安全等级，我们就能看出它整体的安全水平。那么怎样才能做好身份认证这个环节呢？这就需要进行系统分析了，这个问题我们在后续的课程中会详细讲解。

## 2. 授权

在确认完“你是你”之后，下一个需要明确的问题就是“你能做什么”。毫无疑问，在系统或者应用中，我们的操作都会受到一定的限制。比如，某些文件不可读，某些数据不可修改。这就是**授权机制**。除了对“你能做什么”进行限制，授权机制还会对“你能做多少”进行限制。比如，手机流量授权了你能够使用多少的移动网络数据。

最原始和最安全的授权机制，一定是你的每一次操作，都经过了管理人员的审批和确认。比如我们申请签证的过程，其实就是一次申请授权的过程。当部分国家的签证策略比较严格时（如美国），那么我们每次出入境都需要重新申请签证，这也就意味着，会有很多的操作需要进行授权审批，其效率肯定是无法保证的（可以想想美国大使馆门前的长队）。

因此，很多时候，我们会定义自动化的授权机制来进行更快速地响应。比如，某些国家会制定免签或者落地签政策，只要符合一定的条件（如拥有中国护照），就能够直接出入境。这就相当于将“是否拥有中国护照”当成了一种授权的规则。同样的，在安全领域中，也有很多成熟的授权策略，如：自主访问控制、强制访问控制等。关于这些策略，在后续的课程中，我们也会进行详细地讲解。

## 3. 审计和问责

当你在授权下完成操作后，安全需要检查一下“你做了什么”，这个检查的过程就是**审计**。当发现你做了某些异常操作时，安全还会提供你做了这些操作的“证据”，让你无法抵赖，

这个过程就是**问责**。

举一个生活中的例子，当你去银行办理业务时，工作人员会让你对一些单据签字。这些单据就是审计的信息来源，而签字则保证了你确认这是你进行的操作，这就是问责的体现。

审计和问责通常也是共同出现的一个过程，因为它们都需要共同的基础：**日志**。很容易理解，所谓审计，就是去通过日志还原出用户的操作历史，从而判断是否出现违规的操作。而问责则是通过日志的完整性，来确保日志还原出来的操作是可信的。想象一下，如果一份日志可以被人任意地篡改，那我们基于这份日志去进行审计，即使发现违规操作，也无法证明违规操作确实发生了，只能是白费功夫。

可能你会产生疑问，你已经获得了授权，理论上这些操作都应该是合法的，那为什么还需要审计呢？当然，如果授权机制能够达到“完美”，那么审计的意义确实不大。然而，我们一直都强调，安全不存在“银弹”，不可能达到 100% 的安全。即使是 1% 的漏洞，也可能造成 100% 的损伤。

在授权中，我们需要平衡可用性和安全性，很多时候都会选择牺牲部分的安全保障，来降低使用成本。而审计是事后的策略，它做的任何操作，理论上都不会直接影响用户，因此，能够做到更全面更严格，也能发现更多的问题。所以，审计这一环节，对于发现安全问题、回溯产生的攻击、完善安全保护体系来说，非常重要。

而问责，是对审计结果的一个保障，有的时候我们也称之为“不可否认性”。一方面，它保证了黑客无法通过篡改日志或者伪造身份，来隐藏自己的行为；另一方面它也保证了，当审计中发现了恶意的行为，需要寻求法律保护时，我们能够提供充分的证据。

从法律上来说，一个企业和应用在遭受攻击时，只能进行被动防御。如果想要主动出击，打击黑客的话，必须通过法律的途径。因此，建立完善的问责机制，能够为企业提供“法律保护”，大大提高企业安全的自信力。

这里你注意一下，一定不要狭义地去理解黄金法则的每个模块。认证不仅是帐密登录，也可以是生物特征识别或者证书等形式；授权不只是基于简单规则的访问控制，基于内容或者会话的检测等也是授权的一部分；审计也不只是简单的翻日志，很多机器学习、异常检测的算法，也都能运用到审计中来。针对不同的数据，不同的访问形式，我们能够采用的认证、授权、审计技术都不尽相同。

换一种方式来概括的话，你可以这么理解：**大部分情况下，事前防御属于认证，事中防御属于授权，事后防御属于审计。**

## 企业安全建设管理

通过学习“黄金法则”，我们可以看到，安全是一个很浩大的工程，涉及各个方面的投入建设。对于任何一个公司来说，建立安全体系都是一个长期过程，因此，我们需要一个有效的管理方案来进行推动。

通过这么些年的实践，我觉得**安全问题需要自上而下的方式去进行管理和推动**。这也是为什么，大部分安全负责人加入企业做的第一件事就是向上教育，只有企业高层理解了安全，才有可能有效推动安全的发展。

正如，我们在开发一款应用时，需要评估功能的优先级，先以有限的资源实现 1.0 版本，然后再逐步进行迭代，不断完善。在做企业安全建设时，我们也需要对发展阶段进行划分，进行合理管理。通常来说，我们会根据周期的不同，制定三种安全规划，在这里，我举个简单的例子，比方说，可以制定 5 年左右的战略规划、1 年左右的战术计划、3 个月左右的操作计划。

战略规划是一个较长期的安全目标，它和企业的长期发展目标相结合，保证安全的发展能够符合企业的长期发展方向。

战术计划会基于长期的安全目标，拆解出详细的任务计划，比如：项目列表、安全预算、人员扩张等。

操作计划则是对战术计划的具体实现，包括人员的分配、资源的投入、进度的安排等。

和产品研发一样，当建立好不同的计划后，我们就能够给予企业的安全建设一个明确的方向，大大降低投入的成本，提高效率。因此，挖掘安全问题，明确安全计划，对于企业建立安全体系来说，至关重要。

## 总结

好了，今天的内容差不多了，下面我来带你总结回顾一下，你要掌握的重点内容。

黄金法则描述的是，在用户操作的各个环节中，我们所需要采取的安全策略。黄金法则的核心内容包括三部分：认证、授权、审计。**大部分情况下，事前防御属于认证，事中防御属于**

## 授权，事后防御属于审计。

毫不夸张地说，所有的安全保护措施或者工具，都是在黄金法则的一个或者多个模块中进行工作的。安全是严格遵从“木桶原理”的领域，只专注于某一个方向必然无法产出最优的结果。因此，我们一定要积极寻找短板，全面发展。

最后，我想说，安全没有“银弹”。只有当可用性接近 0 时，我们才有可能接近 100% 的安全。比如，将电脑关闭电源并深埋地下。所以，在实际进行安全防御的时候，不要过分追求完美，先有基本的保障就可以了。

## 课后思考

最后，给你留两道课后思考题，你可以选择其中一道来回答。

1. 通过今天的学习，你可以尝试分析一下，你负责的系统和应用中，在认证、授权和审计方面，分别做了哪些工作？又起到了怎样的保护效果？
2. 我在前面说了，安全问题需要自上而下的方式去进行管理和推动，这只是我个人的观点。结合你们公司的实际情况，站在你的角度，你觉得你们公司应该如何去推动安全建设呢？

欢迎留言和我分享你的思考和疑惑，也欢迎你把文章分享给你的朋友。我们下一讲再见！



点击查看 

## 来参加打卡，攻克 工作中 80% 的安全问题



PC端用户扫码参与



新版升级：点击「 请朋友读」，20位好友免费读，邀请订阅更有**现金**奖励。

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 01 | 安全的本质：数据被窃取后，你能意识到问题来源吗？

下一篇 03 | 密码学基础：如何让你的密码变得“不可见”？

### 精选留言 (15)


 写留言



攻城狮Ra

2019-12-11

目前公司主要是通过加密服务器进行认证和授权，通过企业微信在网上办公，工作文档也都是上锁的，由于职务限制审计目前还没接触到，可以说句题外话，公司今天正好停电了，发电机发电之后服务器还是一直连接不上，运维修了半小时才好，可能是服务器老式。

我觉得应该由部门BOSS跟上级反应，最好跟员工再简单培训下，公司现在纯IT的其实...  
展开 

作者回复: 断电恢复其实挺考验运维能力的，也是可用性需要考量的范围。除了引入断电保护的一些设备（如ups，发电机），最好还能够定期进行演练，来验证这些设备是不是真的有效，以及有哪些点是疏漏的。



2





**fgdtz**

2019-12-15

你好老师，关于APP与服务器沟通安全我有个问题，望老师能解答。

api请求认证或加密一般都有key等，硬编码在APP，而APP有被反编译的风险，放c++ 编译成SO库，虽加大了安全系数，但黑客可直接用这SO库即可，而调用的逻辑，反编译代码里也有，如何安全存储？

展开 ∨

作者回复: 你好，感谢你的留言。如果是加密数据的话，用非对称加密即可，公钥可以公开，直接存储到前端即可。如果是第三方api请求认证的key，一般是不在前端调用，而是后端去进行封装。



💬 2

👍 1



**西西弗与卡夫卡**

2019-12-11

我们是SSO加权限控制，再加事后审计。

展开 ∨

💬

👍 1



**一步**

2019-12-10

任何领域都没有银弹的

展开 ∨

💬

👍 1



**二马**

2019-12-18

安全遵循“木桶理论”，这个在实践中有时候会被误解，安全涉及的领域很多，是无法做到每个场景都要把短板提高，有些做到基本防护已经可以解决安全问题。所以，安全加固，先做好安全威胁建模，把影响最大，最可能被利用的威胁降低，即把这些威胁的安全防护之板做到极致，而不是纠结于短板不够好。

展开 ∨

💬

👍



**niuniu**

2019-12-17

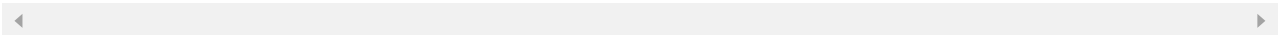
为什么说“我知道什么”是强度最弱的认证手段？有些书认为这是最强的认证手段，而“我是什么”是最弱的。我觉得还是有道理的，因为“我是什么”是无法改变的，而我

知道什么是变化莫测的，只要有共产党员钢铁般的意志，即使是严刑拷打也无法得到他知道的。

展开 ∨

作者回复: 你好，感谢你的留言。从个人角度来说，这么理解是没问题的。但对于普通应用来说，更多的是需要考虑普遍现象，即大多数用户不会设置强密码，也不会有较强的安全意识和坚定意志，对于这部分用户来说，“我是什么”是成本最低，安全性最高的解决方案。

对于比较专用的系统来说，比如军方系统，肯定还是会以“我知道什么”为准，因为军人安全意识高，不会泄漏密码。而“我是什么”作为一种半公开的信息，泄漏的可能性对于军人来说，更高一些。



**Cy23**

2019-12-11

安全原则，如何入手去解决安全问题，安全是相对安全没有银弹。



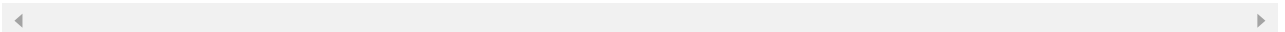
**追风筝的人**

2019-12-10

SSL VPN用户在访问虚拟站点的时候会被radius服务器进行AAA认证 授权 审计。radius认证方式有2种 PAP认证即用户名密码认证，用户名是明文保存的，密码是MD5加密的，第2种是challenge认证 会有2次认证第一次用户名密码认证，第2次challenge动态密码认证。2次认证的比只有1次的radius认证安全级别高。1812端口负责认证授权，1813端口负责审计，radius客户端充当NAS网络接入服务器和radius Server交互 对用户行为做出响应的...

展开 ∨

作者回复: 不好意思，Radius认证只是学习过，并没有在工作中接触过。所以没办法回答你关于最佳实践的问题了。。。



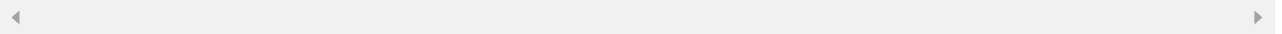
**张诚**

2019-12-10

为了遵循CIA的安全原则，我们可以从哪些方面去做，认证，授权，审计这三样是对机密性，完整性的实现。在认证模块，我们系统采用的统一的鉴权中心做系统间调用的鉴权操作，在开发的项目中，授权采用的是开通产品很渠道，是数据库内进行的配置，审计是在系统的整个功能调用中加入日志记录

展开 ∨

作者回复: 赞



💬 1



**link**

2019-12-10

银弹效应：妄图创造某种便捷的开发技术，从而使某个项目的实施提高效率。又或者指摆脱该项目的本质或核心，而达到超乎想象的成功。银弹在现实生活中是指能够解决棘手项目或者一件不可能的事情的方法或者技术手段。

展开 ▾

作者回复: 你好，感谢你的留言。帮我解释了一下什么是银弹。首先，银弹是国外的说法，我知道的大概起源就是银弹可以打死所有吸血鬼，所以人们用银弹来比喻解决一切问题的方法。



💬 1



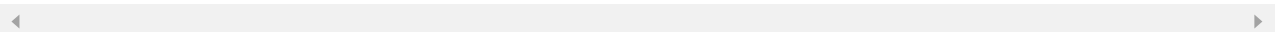
**米小亮**

2019-12-10

安全问题从三个层面：

- 1.国家立法，建立标准
- 2.企业根据法律和标准，实现自己的安全目标和政策
- 3.个人首先遵守标准和制度，其次是培养安全意识

作者回复: 嗯嗯，这是比较宏观的安全层面了。



💬



**小晏子**

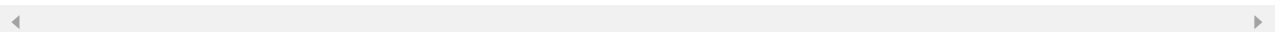
2019-12-10

对于安全建设的问题的一些考虑：

- 1，首先保证公司基础设施的安全性，做白名单访问机制，密码认证等
- 2，其次是对公司成员的权限做细化，分出权限等级，比如哪个group的用户可以做添加删除操作，哪些group只有访问权限等
- 3，对于所有的web访问强制使用https...

展开 ▾

作者回复: 这是一些细节点，可以根据课程进度，一步步梳理，成体系化





**许童童**

2019-12-09

老师讲得很不错，安全中的黄金法则，大多数系统都是按照这个法则在执行的，一些安全问题最后的原因也可以归纳为黄金法则的这三个阶段之一，另外，一定要注意安全是遵循木桶原理的，不要一味的专注某一个方向。最后，安全没有银弹，加油。

展开 ▾



**星亦辰**

2019-12-09

大佬解释下，双因子认证是什么意思？解决的是什么问题。认证，授权，审计除了依靠日志还有没有别的办法？

展开 ▾

作者回复: 双因子认证，就是通过两种不同的方式来共同认证。比如之前网银交易的时候，既需要支付密码，也要u盾的一次性口令。现在可能这种显性的双因子可能不多了，因为都把手机这个设备当作可信环境来作认证了。



**Chocolate**

2019-12-09

我们采用 SSO 的登录方式，SSO 登录时对用户名和密码进行校验，SSO 通过在用户多次输入错误密码进行处理、每三个月更换一次密码（后台系统）等方式来加强认证的安全性；在业务系统中，用户的大部分操作都会对具体的权限进行验证；操作会以日志的形式进行记录。这样基本保证了用户和数据的安全，而且有些操作需要回溯的时候也能查到谁操作的、在哪个时间点操作的、操作了什么。...

展开 ▾

