**安全世界观**

**黑帽子、白帽子**

白帽子： 指那些精通安全技术，工作在反黑客领域的专家们。  
黑帽子： 指利用黑客技术造成破坏，甚至进行网络犯罪的群体。

对于黑帽子，只要找到系统的一个弱点，就可以达到入侵系统的目的；对于白帽子来说，必须找到系统的所有弱点，不能有遗漏，才能保证系统不会出现问题。

从对待问题的角度，黑帽子为了完成一次入侵，需要利用各种不同漏洞的组合来达到目的，是在不断组合问题；而白帽子在设计解决方案时，如果只看到各种问题组合后产生的效果，就会把事情变复杂，难以细致入微地解决根本问题，所以白帽子必然是在不断地分解问题，再对分解后的问题逐个予以解决。

**安全的本质**

被划分出来的具有不同信任级别的区域，称之为信任域，划分两个不同信任域之间的边界，称为信任边界。

数据从高等级的信任域流向低等级的信任域，是不需要经过安全检查的；数据从低等级的信任域流向高等级的信任域，则需要经过信任边界的安全检查。

**安全问题的本质是信任的问题。**

一切的安全方案设计的基础，都是建立在**信任关系上**的。 我们必须相信一些东西，必须有一些最基本的假设，安全方案才能得以建立；如果我们否定一切，安全方案就会如无源之水，无根之本，也无法完成。

一旦我们作为决策依据的条件被打破、被绕过，那么就会导致安全假设的前提条件不再可靠，变成一个**伪命题。**  
把握住信任条件的度，使其恰到好处，正是设计安全方案的难点所在，也是安全这门学问的艺术魅力所在。