非官方辅导资料，如有错漏、纯属正常。（作者 QQ/WeiChat：9201491）

CISSP必过葵花宝典2017

基于 Official (ISC)² Guide to the CISSP CBK, 4th 英文版翻译（**CBK_4**）

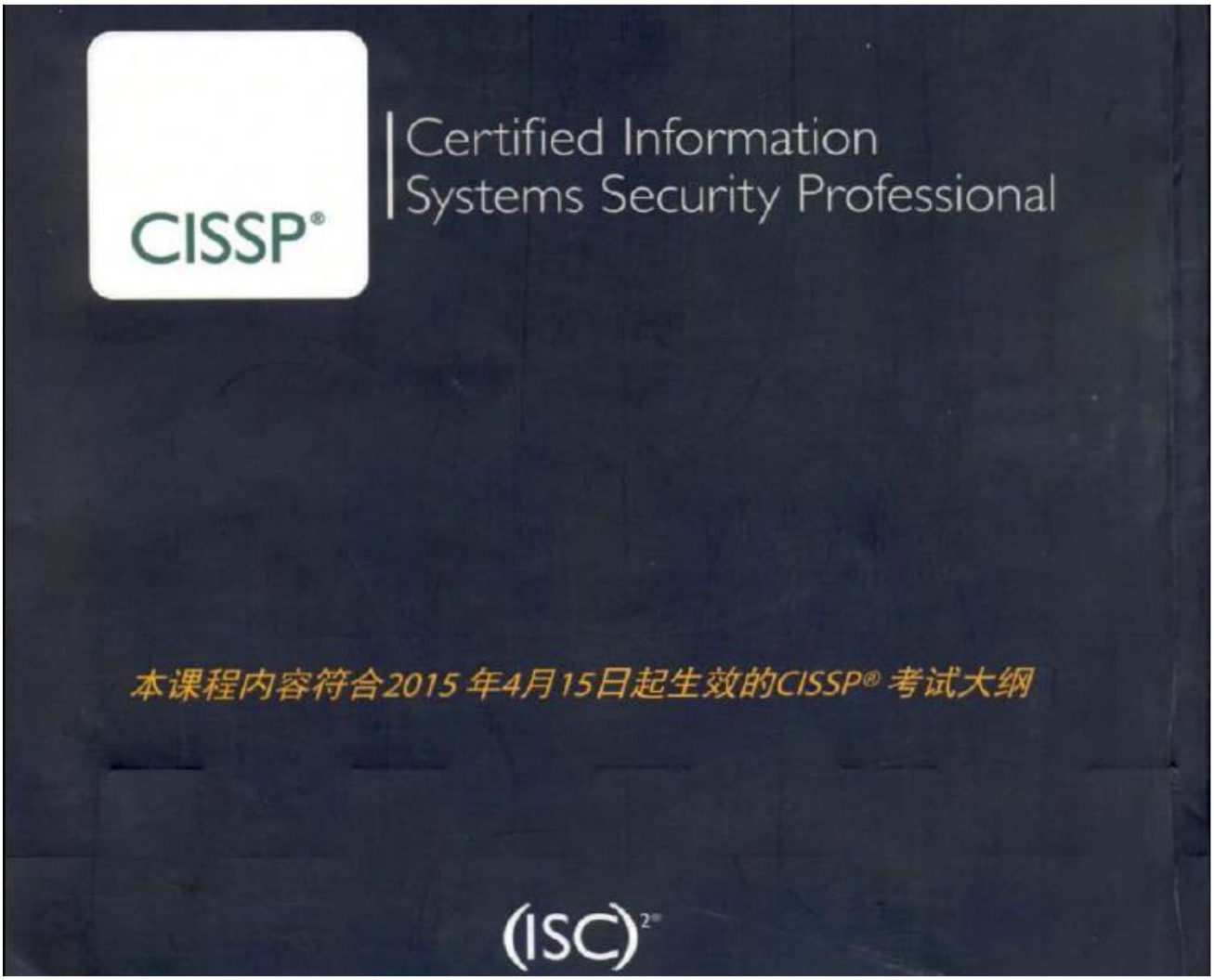
根据 CISSP Official Study Guide, 7th（**OSG_7**）和

CISSP All-In-One Exam Guide, 7th（**AIO_7**）进行补充完善

参考 CISSP All-In-One Exam Guide, 6th（**AIO_6**）中文版规范措词

结合官方习题集、历年真题和 Certpass、TestKing 最新模拟题对考试要点、难点进行归纳

2017.02 版



目　录

前　言

(ISC)²是一个注册商标，读作 ISC-Squared，是 6 个首写字母 IISSCC 的缩记，其全名是：The International Information Systems Security Certification Consortium，中文名是：国际信息系统安全认证联盟。它是全球最大的信息、网络、软件与基础设施安全认证会员制非营利组织，是 CISSP 认证考试的管理机构。

一、考试介绍

CISSP 考试是面向管理的，技术要求并不高，但要求知识面广，即“一英尺深一英里宽”。

1.考试的特点

①**全面**。8 个域的内容什么都会考，随机抽取，没有重点，但是有的知识域（章节）出题权重(数量)比较多。从准备角度来看，必须掌握大纲、教材或辅导书里的全部知识点；从做题角度来看，押题或收集真题是没必要也没意义的，官方的章节练习题、测试习题都很好的覆盖了知识点以及题型，且考试不会出现曾经做过的一样的题，但做好了习题集就一定能过。

②**基础**。考试没有技术难度大的分析，不研究具体的算法和协议，只要求理解各种模型、标准、算法、协议、流程的优缺点、应用方法与要求等，有计算机基础的人肯定看得懂。目的是知道该用什么技术来解决什么问题，而不是钻研某个技术的详细实现。大量考题都是在一个设定的场景里考基本的理论。

③**有限**。考试内容一定在 CBK 或者官方指定教材中，绝不会超出；据不完全统计，按照考试大纲，8 个域共有 65 个章节(模块)、198 个小节(要点)、1486 个知识点(考点)。

④**交叉**。大部分知识点并不是独立的，是互相关联、综合运用的，必须通过反复阅读和归纳总结来理清关系，建立知识体系，清晰的掌握相关联知识的应用领域、应用场景和方法。

⑤**离散**。CISSP 的通过率不高，不是我们不聪明，是没有中文版本的成体系的、全套的、完善的教材、辅导书和习题集，而且任何一本书都没有 100%的覆盖和详细描述 1486 个知识点，也没有把各章节的知识点关系串联起来，准备考试要花大量的时间去收集资料、梳理资料、理解资料、形成笔记，而且好资料全是英文版本的（中文的除了 AIO_6 和 OSG_7，其它的翻译都很滥，习题翻译更烂）。现在知识点都整理好了，过与不过全看你做了没做。

⑥**跑偏**。考试中出现的难题，一般是教材中没有详细讲述但 CBK 里有列举的知识点，或者是自己了解比较少的、不常用的标准/法规/协议/模型/流程等内容，总之要想考过，必须老老实实花时间来积累知识，攻克隐晦难懂的外国的标准/法规/协议/模型/流程。这里要强调的一点就是：不管你是科班出身还是半路出家，CISSP 对都是一个全新的知识领域，很多内容是可以和工作经验相关联，但绝不是你曾经学过的那些技术知识，一定要研究透它的知识体系。

⑦**易错**。做错题一般不是因为自己技术不好、理论不扎实，而是因为：看错题干；对自己工作领域以外的知识掌握不牢；按经验做题，没理解题目的出处、原文或考的知识点是什么；没建立知识体系、不理解美国思维，肯定会错；英文不好，不能从超滥的中文翻译反推出英语原文，肯定会错（看不懂英文原题也肯定会错）；逻辑不清晰、思考不仔细肯定会错（做完一半/150 题/3 小时，大脑就疲劳了）。考题的很多技巧与英语六级阅读理解题是完全一致的，必须理解题目的知识点、回忆到教材的原文出处，千万别扫一眼题目和答案就胸有成竹的作出选择，要看清问的是什么，考的是哪个知识点，所以英语阅读理解的技巧是同样适用的，如：

有 any、only、every、must 等绝对性的描述肯定不对；文字最长的选项就是答案；在对立的选项里 2 选 1；字面很像的选项很可能是干扰项等等。

⑧**没用**。应试和运用是完全不同的，考过了这个证还是什么都不会，仍然成不了技术专家；当然，有这个公认的含金量高的认证，是一种认可，方便找工作和升职，而且学习过程可以梳理构建自己的知识体系，知道如何构建和运营一个完善的安防体系，也能结交人脉，对于提升综合能力有很大帮助。就像考驾照一样，考过了就有资格开车上路了，但你还是不敢马上独立跑高速、跑长途，必须搞台车练练手，才能成为老司机；相反，很多老司机常年跑车，但让他去再考一次驾照，不好好准备肯定过不了。技术高手不需要证书来证明，而且技术高手考试的通过率还都不高，因为他没有掌握考试的精髓。相反，管理人员的通过率高些。

2.通过考试的必要条件

①**信息**。自己收集、整理相关的资讯和学习资料；搞清楚怎么约考、怎么背书、怎么维持 CPE 就行了；很多收费的资料都可以在网上找到免费的下载，但资料搞全后，就没必要浪费时间上网了（其实是在看电影、打游戏），需要上的网站只有几个，在汇编资料里有网址。

②**精读**。选择最新最全的 1 到 2 本教材，理解到每一句话，必须总结归纳出自己的学习笔记，该宝典就是作者边学边记的，不整理自己的笔记，就不能牢固的建立起自己的知识体系，碰到题目就不能快速查找资料，就没有一个辅助复习和方便查阅的知识要点集。这是一个从薄到厚，再从厚到薄的过程。

③**做题**。很多考点书上讲的不多、不全、不细，全靠做题来巩固。而且必须通过做题来理解它的出题思路和答题技巧。作者因为记忆差，考前把 8000 多道题反复做了 4 遍，复习半年后，3 小时可以轻松做 250 道题；当然，绝世高手可能不做题也能过。

④**英语**。看中文效率最高，以中文为主来看书是可以的，但最好扎扎实实看点英文资料，做大量英文题，因为很多考题的翻译很烂，需要看英文术语、用英文思维才能准确理解题干、判断混淆项和最佳项，而且考试真题的简体中文翻译也不符合我们平时学习的思维和表述。作者的知识体系全是用中文建立的，但做题只做英文题，做中文题实在难受，还会产生误解。建议：主看中文书学得最快，辅看英文书加深理解，只做英文题准确无误。

⑤**培训**。通过考试只能靠自己大量的学习和积累，培训班的作用是提供最新的中文资料，提供答疑、报名、背书和 CPE 维持服务，并不能用五天时间把知识全部塞进你的大脑，但可以介绍方法、思路、规则，提高你的学习效率，节省收集、整理的时间。其实，作者和身边的同事是同时参加了谷安、汇哲、爱思考、天融信的几个培训班，算是搞明白了，不过如此。我身边的人很多都没有时间听完全部的培训课程，而在线视频更是没一个人完整看下来了，我自己几十 G 的视音频资料从没看过，只要看 3 本书，做几千道题就够了。有了葵花宝典，你可以自己积累，钻研半年你也可以成为讲师了，不报班也能过。

报还是不报培训班，是个很纠结的问题，这里多说几句。如果有钱，肯定是报，某培训班研究 CISSP 很深入，全程服务也很细致。如果没钱，自学也完全可以通过，只是后续背书、CPE 维持挺烦琐的。还是举考驾照这个例子：现在国家新政策允许自学考驾照，不用再报驾校了，如果有一台车练手，按教程练肯定能不花钱轻松考到驾照，但如果对考场规则和流程不熟，而后续还有违章处理、上牌年审、保险理培什么的事，自己搞定是省钱了但费时伤神，花钱搞就省心了。不管报不报，花点小钱把资料搞齐还是可以的，相当于有台练手车，等熟练了，再决

定下一步怎么搞。

⑥**自信**。别想作弊、代考、押题什么的旁门左道了，从事安全行业，尤其是进入高层，必须具备最基本的职业道德和个人素养。

⑦**时间**。万事俱备，就差积累，最好封闭式学习，排除干扰，作者白天上班，晚上陪小孩家教再哄小孩睡觉，半夜 11 点到凌晨 2 点学习，坚持了 8 个月。

⑧**评测**。3 次闭卷模拟测试全部 80%正确率以上，就可以考试了。（有的培训班题目比较老旧，会要求学员模拟测试 90 分以上才能正式考）

⑨**考试**。内容熟悉的人，基本上 4 个小时以内就全部做完了，做的慢的都是模棱两可，知识不牢的人。总之，考试分数和复习时间成正比。做一个复习计划，然后按部就搬的执行就行了，过与不过全在于你做了没做，看你有多大的决心了。如果给一个标准的化，我认为，大部分人需要不间断学 2 小时×120 天就差不多了，基础较差、拖拖拉拉的人可能要 1 年以上。

3.考试体验

①**时间**。约考不用太早，基本上提前个半个月预约就行了，会有考位的，约早了肯定准备不充分，总会纠结要不要延迟考试（50 美元/提前 24 小时改签），当然也可以早点约考，给自己一个明确的期限，倒逼自己抓紧时间。我是考前休假一周，每天一次连续完整的 250 题模拟考试，有把握通过了，才定的考试时间。模拟考中文题，一般 3 小时内完成；考英文题，一般 4 小时内完成。实际考试是简体中文，但全靠看英文对照做题，4.5 小时完成；中间自由休息几次；最后一个小时从头到尾把所有题检查了一遍，更正了 6 道题。考试时间绝大部分是上午 9 点到 15 点这个时间段，我约的是中午 13 点到 19 点这个时间段。如果上午考，早上准备工作仓促，路上拥堵奔波、人犯困，到了中午没饭吃，又饿、更困。如果下午考，有一上午时间轻轻松松慢慢做准备，在楼下吃个午餐，我还把葵花宝典完整看了一遍，然后提前 10 分钟到考场拍照、录掌纹。做完 150 道题，出来喝水撒尿；做完 250 题，又出来喝水撒尿，还跑楼梯间抽了根烟；最后一个小时完整检查了一遍，心想肯定过了，交卷走人，当场打印了成绩单。然后就约人吃火锅去了。

②**系统**。考试系统和考驾照科目四的理论考试系统差不多，和计算机等级、职称英语等很多机考的考试系统都差不多，界面看上去是很过时的、老旧的程序风格，字体也很粗糙，菜单和功能相当的简单，右上角显示剩余的时间和完成的题数。做题是不能跳着选做任一题的，必须从头到尾逐个的做，因为你除了点击答案，只能点“上一题、下一题、做标记”3 个按钮。老老实实一个一个的做，挺枯燥的，头昏眼花，如果不是长期加班学习和多次模拟考的磨练，根本坐不住 6 个小时。等全部做完 250 道题，才出现检查题目的功能菜单，可以比较灵活的选择性的检查做题了。检查题目支持 3 种方式做题：一是全部从头到尾检查，二是只显示做了标记的题，三是自己随时可以点击“检查”按钮按需选择要检查的题。

③**真题。**考试的真题没有和做过的练习题是一样的（老外确实用心出题了，题库保密工作还做得挺好）。真题仍然是大量的管理类、理论性、概念性、理解框架模型原理流程方法的题，虽然内容都很明显在考试大纲范围内，但很多的具体知识点的描述并不是熟悉的中文教材、辅导书里的原文；有的是在 CBK 或 NIST 800 系列特别出版物中有类似的描述；有的是在特定场景里的实际情况。如果不好好看书，归纳出学习笔记，光靠题海战术也是过不了的，何况 CISSP 没有一套像样的中文习题集（“天龙八部”里汇编了 3410 道中文练习题，我都很不满意，还

是要靠做英文题来积累和巩固）。250 道题，总共约有 3 道排序题、3 道拖拉匹配题、3 道图片点击选择题；其余全部是单选题。绝大部分是题干不长，就问 2 句话的简短问题，约有 200 道；还有 50 道是情景题，就是先描述一个场景，然后告诉你后面的 3 道题都是基于这个场景的；而且，每间隔 20 道普通简短题，就会出一道情景题，这个规律和节奏还是很稳的（情景题一定要小心，不然一偏差就会连错 3 道）。真题的中文翻译虽然是经过了审核校验的，但我还是一头雾水，所以全程都是点开英文来做题。感觉考试题是由香港人翻译成中文的，比如 organization 考试中翻成“机构”，教材中翻成“组织”，erase 考试中翻成擦除，教材中翻成清洗，还有好多差别不记得了。而且很多题前后有关联、暗示的关系，做到后面，会启发到原来前面那个题应该是这样的。所以必须留时间检查题目。

二、宝典内容

葵花宝典的核心是要点笔记，是一系列的资料汇编和整理（培训班的内部资料是没有的），包括 CISSP 必过三部曲：

1.九阴真经（知识之源）：最新的、最权威、最全面的官方的学习资料汇编，大部分已经是中文了。这是最基础的资料，英文中文都要看，反复看；先粗看后做题，做了题知道差距后再精看；最后就可以不看了，内容都吸收理解到学习笔记里了。包括：

①书籍（好多）

▲考试大纲中、英文版/Exam Outline,Candidate Information Bulletin-2015（**CIB**）▲CBK 官方指南_第 4 版中英文/Official (ISC)2 Guide to the CISSP CBK, 4th（**CBK4**）▲CISSP 官方学习指南_第 7 版/CISSP Official Study Guide, 7th英文版（**OSG7**）▲CISSP 认证考试指南_第 6 版/CISSP All-In-One Exam Guide, 6th中文版（**AIO6**）▲CISSP 认证考试指南_第 6 版/CISSP All-In-One Exam Guide, 6th英文版（**AIO6**）▲CISSP 学习指南一步登天/11th Hour CISSP Study Guide▲CISSP 预习指南黄金版/CISSP.Prep.Guide.Gold.Edition.Wiley▲CISSP 内训核心辅导书/Study Guide, Third Edition-2016▲CISSP 必考要点笔记/CISSP Comprehensive Review Notes-2016▲中文资料▲备考经验介绍一大堆

②课件（共 8 套）

▲中文培训讲义 8 个域 2016▲知名机构 CCCURE 的新版培训课件 8 个域 CBK4_2015▲美国 CISSP 特训班完整讲义（1500 页）▲官方中文培训讲义 10 个域 2013▲国内培训机构自制讲义 10 个域 2013▲AIO 中文培训课件 10 个域 2013▲AIO 英文培训课件 10 个域 2013▲Shon Harris (CISSP all in one 的作者)编写的 CISSP 讲义▲中文思维导图全集▲英文思维导图全集

③视频（共 5 套）

▲10 个域中文培训辅导视频全集 2013▲8 个域英文培训辅导视频全集 2015▲美国 5 天特训班完整培训视频全集 2015▲美国知名机构完整培训视频全集 2015

④音频（共 3 套）

▲国内机构中文 5 天培训完整音频全集 2015▲美国 5 天特训班完整培训音频全集+讲义+习题 2015▲知名机构 CCCURE 的新版培训录音 8 个域 CBK4_2015

2.葵花宝典（去粗取精）：全部知识点的梳理。按照考试大纲的结构，把各大权威资料的知识点进行汇总，梳理成知识笔记，覆盖率达到 95%以上。学习过程就以该笔记为基础，边看书、边自己理解，再整理完善这个笔记；精读完几本官方教材后，就可以甩开书了，以笔记为

参考，大量做题，用好 Word 的导航窗格、PDF 的导航标签以及内容搜索功能，可以快速找到任一考题的知识点；做完各章节的题，基本上就建立知识体系了，就可以冲刺复习，做 N 套综合的模拟考试题，把笔记里已经掌握的知识逐步删掉，只留下需要重点回顾记忆的知识，最后就变成一个小册子了，考前好好过一遍就可以进考场了。为了方便学习，该宝典提供完整的 Word 版本，可以自行编辑整理。（友情提示：该宝典的内容仍有部分错误和偏差，复习过程中自己去感受、修正吧，模棱两可没把握的知识点一定要自己去查验核实）

3.天龙八部（百炼成仙）：2016 年以来的最新的、最权威、最全面的官方的习题集汇编（精品题库 12000 道，备选题库好多好多套）。其中核心题集涵盖了 AIO、OSG、CBK 和官方出版物的最有价值的习题共 7812 道（其中中文 3410 道，真题回忆 640 道）；整理的 2016 年综合模拟测试题共 10 套、3380 道；全部都有答案解析，不用来回翻看几本书、到处查找答案，而且知识疑惑直接在葵花宝典里可以找到原文。当然，AIO7 附带的练习题光盘（1629 道选择+90 道拖拉匹配）和 OSG7 提供的在线练习题（1400 道，拖拉、卡片各种形式）是非常好的学习资源，也有必要做，做完必过。关于 PDF 题库的使用方法：用 PDF 编辑软件看书和习题（ACROBAT 什么的），用下划线、加色等方式可以注释笔记、选择答案和做过的题，比用纸质书的效率要高。（此外，第二梯队备选题库，汇总了国外知名的英文模拟题和 2015 年以前的各大中文题集等，如果精力旺盛看看也行）汇编前的原文题库有：

▲CISSP Official ISC2 Practice Tests 官方指定习题集及解析（2016 出版备考必看）

▲CISSP Practice Exams 最新官方习题集第四版（2016 出版备考必看）

▲Certpass.CISSP 最新模拟题集 V2016-01-04

▲CISSP 正版题库 TestKing.v10.245Q

三、培训机构

2013 年起，考试已经是简体中文；OSG7 中文版已于 2017 年出版；知名培训机构也研究撰写了大量中文资料和测试题；CISSP 的应试难度将有所下降，通过率和持证人数应该会大幅提高。关于培训班的对比，本来详细列了很多对比，算了，不说了。**关于通过率：**瞎猜测 2016 年全国约考人数 398 人，参加考试约 304 人，第一次通过约 207 人。

四、主流教材

可以作为学习教材或辅导书的只有 OSG、AIO、CBK 这 3 本，其它的精品英文书籍也很多，中文讲义也很多，可以做为补充资料、参考资料，CBK 的内容比较全、但看得难受，其它都不全，但容易理解。葵花宝典的内容是全面而且高度归纳的，没有精读过教材直接看宝典很难快速理解透，每一句话都有大量的信息，这是一个学习和思考的过程。建议：

①精读 OSG7_2 遍，搞定这一本就够了，边看边梳理葵花宝典笔记；

②通读 AIO6 中文版和 CBK4 中文版各 1 遍，边看边完善笔记，补充、巩固知识点；

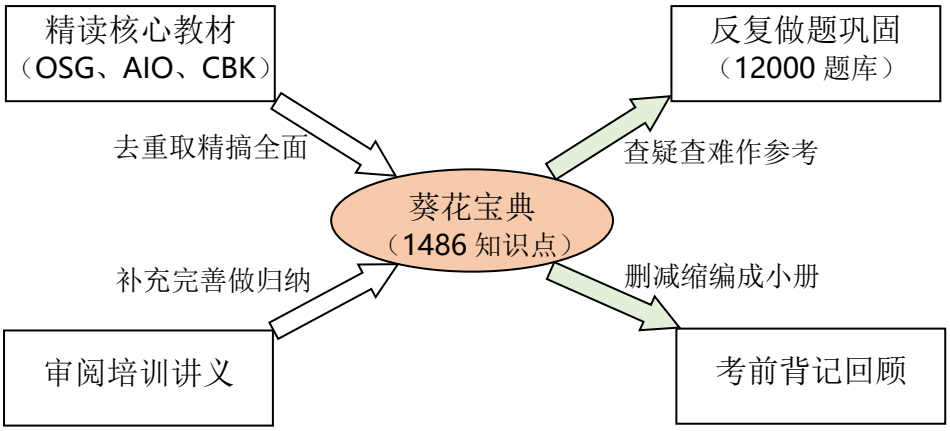
③阅读 AIO7 英文版新增的内容，继续完善笔记；

③审阅 1 遍中文 PPT 讲义，继续完善笔记（如果报了班，就在培训时边听边完善笔记）；

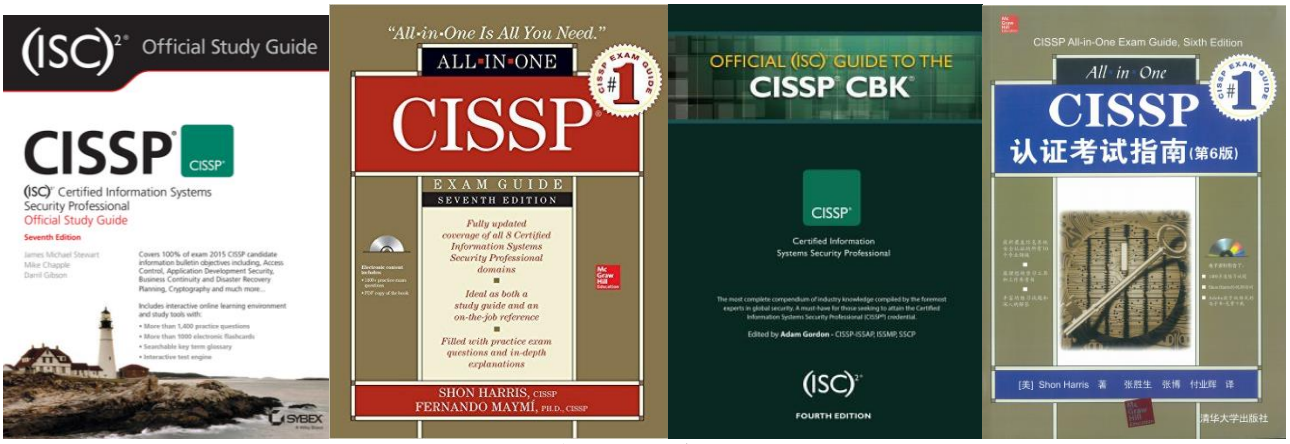
④学完做题，做完再学，学完再做。

作者采用的是学习方法是“一看二记三做题，查漏补缺模拟考”，先看中文书学的快，只做英文题理解透，属于笨鸟型学习法，对于学霸型人才，肯定有更高效快速的学习方法。

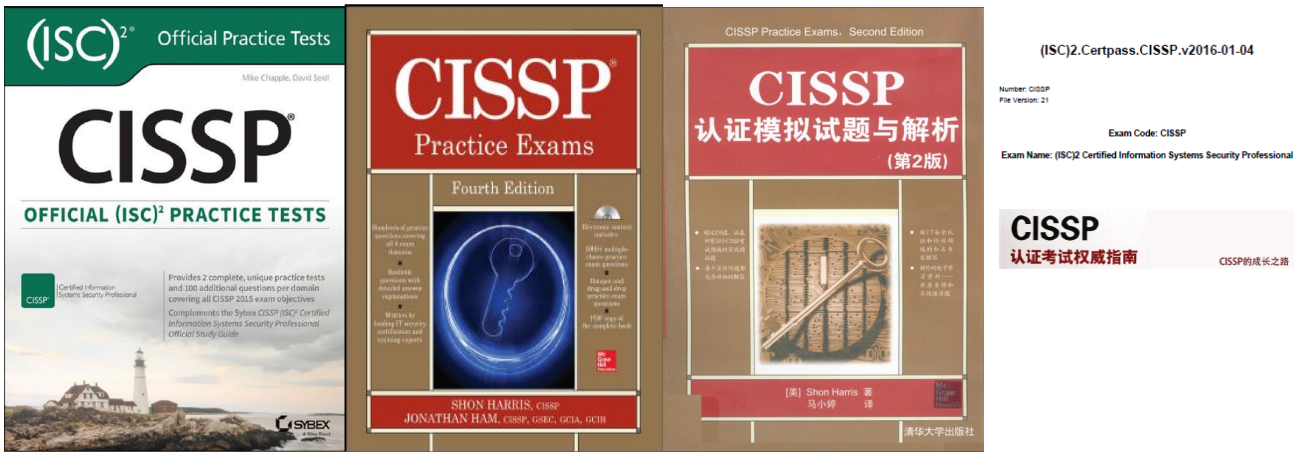
关于葵花宝典的作用与方法，下面这个图可以做个参考：



教材按重要程度排序：



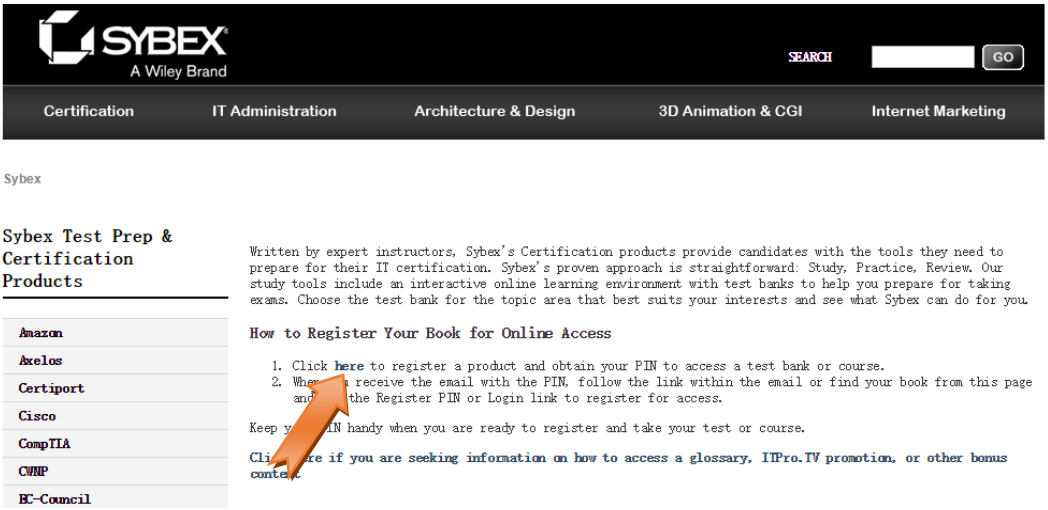
常用习题集：



OSG7 在线练习题的注册方法：

OSG7 书上的网址是错的，可以登陆 www.wiley.com/go/sybextestprep 注册，根据提示回答问题就行了。也可以登陆 sybextestbanks.wiley.com，

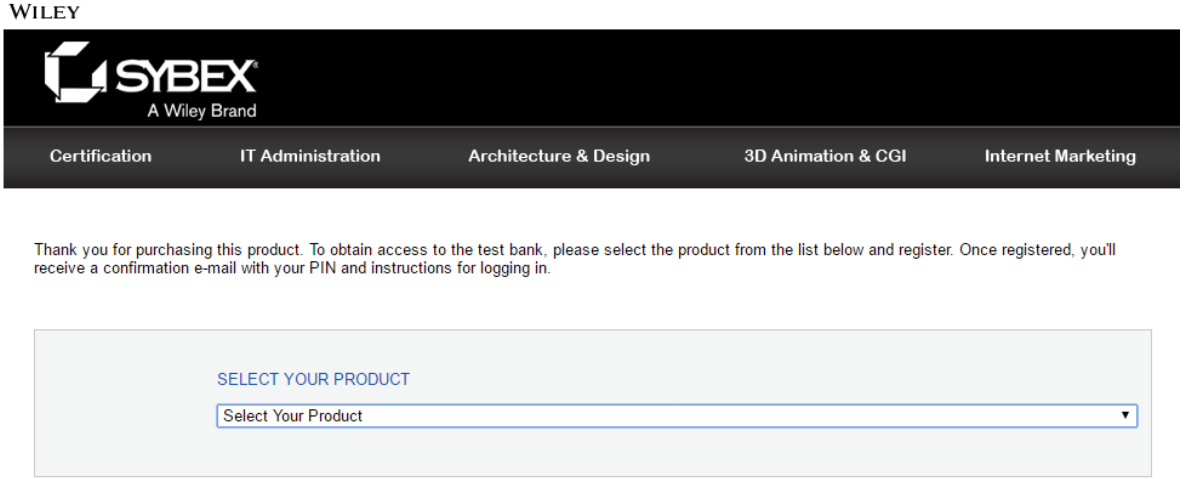
或 http://sybextestbanks.wiley.com/course/index/id/102，选择 ISC2，即进入在线学习，要先注册。点击 here 就可以进到注册页面了。



注册使用在线练习题：

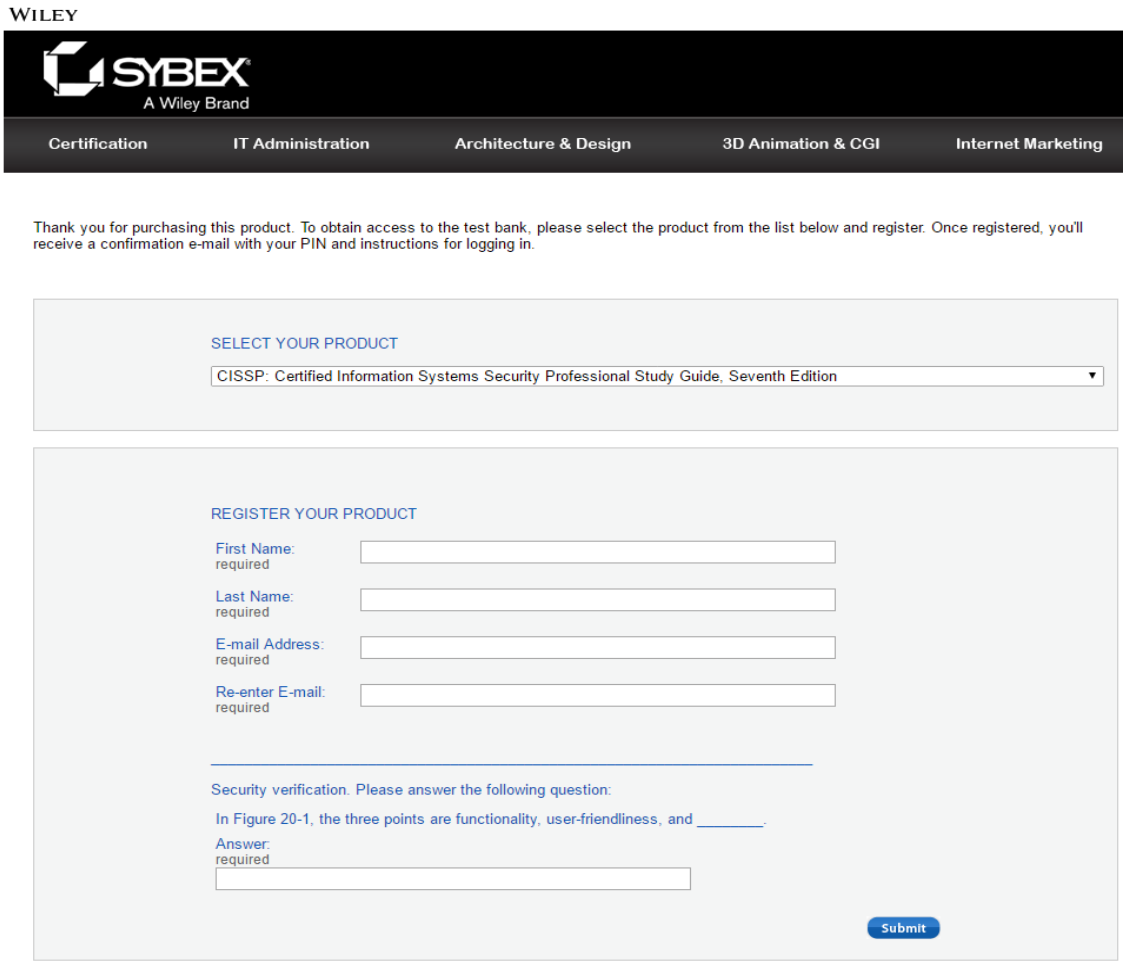
页面 1 地址如下，选择 CISSP Study Guide 7th 这本书就行了，自动进入页面 2.

http://customer.wiley.com/CGI-BIN/lansaweb?procfun+shopcart4+SH4FN19+funcparms+PARMKEYG%28A0060%29:SYBEX



页面 2 地址如下，填写资料并回答一个关于书本内容的验证问题，就 OK 了。

http://customer.wiley.com/CGI-BIN/LANSAWEB?WEBEVENT+R0E37314884A6B8014146071+PRD+ENG



上面讲的乱七八糟的，其实只要搞对网址，内容都看得懂，都有提示。

另外就是 AIO7 附带的光盘习题 1692 道，是非常接近真题的。

五、知识简析

老外干什么事情，最喜欢的就是标准化思路，按科学的套路来。先搞清楚原理、机制，然后制定出一套标准/框架/模型什么的；然后遵循这个标准/框架/模型，根据实际需求来拟制出完善详细的策略/方案/计划；接着就按计划通过一系列的管理/治理/运营的方法手段来实施和执行各项具体的工作；还要对完成的每项工作或者产品进行测试评估和认证认可才能接受或验收；最后根据业务的完成效果再来修订标准/框架/模型。为什么要搞架标准/框架/模型呢？这就是“标准化”观念，可以实现高效协同、量化管控、避免误解。

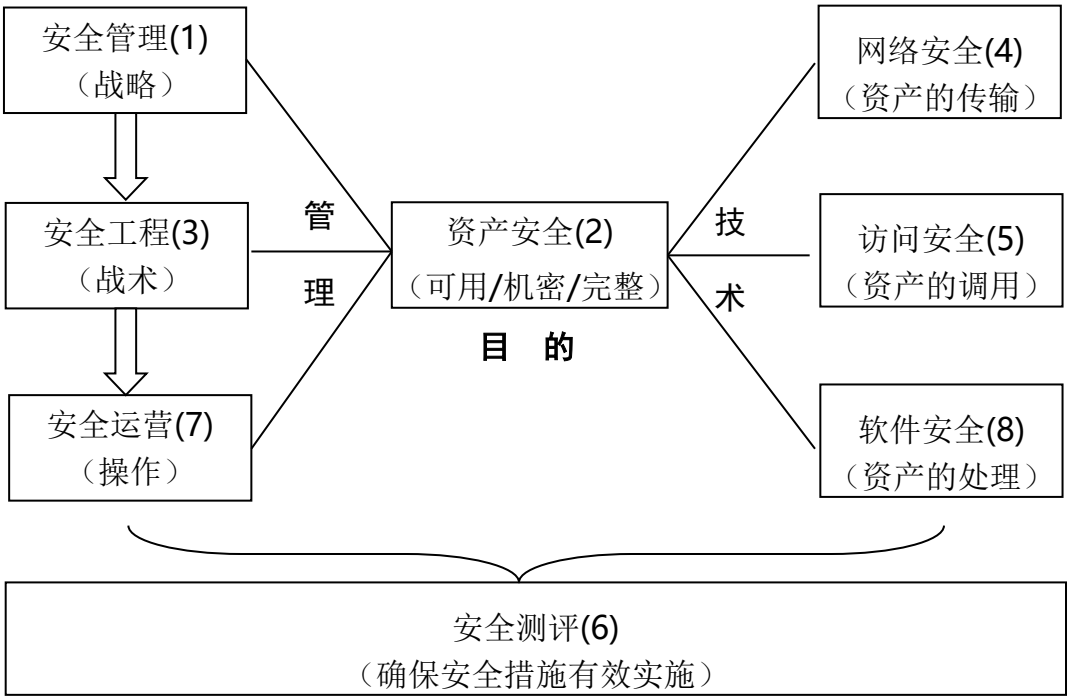
针对 CISSP 的应试，基本路子就是要通过学习充分理解其 CBK 的内容，建立起自己的信息安全知识体系。在全部 8 个知识域中，各域的层级不同、方向不同、相互关联。通过学习建立起自己知识体系的一个重要标志就是：看到任何一段内容或题目，能快速反应，知道它对应于 CBK 或考试大纲里的哪章？哪节？或者对应于教材里的哪个知识点，这就是有的放矢。当然，知道那么多点知识点的位置出处还不够，还要理解它的内容（需要大量时间积累）。建议先初步建立起知识框架，再仔细理解所有内容细节。

1. 知识框架

属于管理范畴的知识域有 3 个，涵盖了信息安全各个专业领域，包括从高管管理到中层组织到基层操作的 3 个层次：**安全管理（即统筹治理）=>安全工程（即组织实施）=>安全运营（即具体操作）。**

属于技术范畴的知识域有 5 个，针对某类信息安全业务工作，包括：**网络安全；资产安全；访问安全；软件安全；安全测评。**

具体看图：



总的来看，8 个域知识可概括为：

从三个层次来逐级抓好安全管理工作；（左）

从三个方面来合力完成资产安全任务；（右）

通过测试与评估来确保工作有效落实。（下）

当然，你也可以从攻与防、安全内核到外部的层级、数据的生命周期、系统的安全需求与安全确认等角度来理解和构建各域知识。

2. 知识概要

①安全和风险管理（安全管理）

这是上层的，讲方法、讲原则、讲策略、讲宏观、讲管理。包括：

*安全的目标：三元组；

*实现的途径：安全治理，治理的方法和思路；

*解决的方案：各种角色分工合作、联动协调；

*实现的策略：策略、指南、操作 3 个层次；

*工作的落实：应尽职责、应尽关注；

*法规的依据：法律、法规、道德的约束；

*管理的核心：把“事”管死，把“人”管活；

*实现安全先要搞清楚风险：包括风险管理的基本要素、概念；还有流程（识别和评估）；也有方法（定量和定性）；还有风险的处置（消减、转嫁、接受）；还有风险管理的架构与威胁建模。

*风险管的再好，也会出现问题，那么业务连续性的工作和灾难恢复的工作必须要做。

②资产安全

*什么是资产：要分类和分级，要搞清关系（资产所有者、监管者）；

*怎么保护敏感资产：就要搞清数据质量，正确的处置和重用数据；

*保护资产的安全措施：保存、传输、使用都要有措施，最低的标准就是基线。

③安全工程

作为一个安全总监，怎么管好一个公司的整体信息安全呢？

*工程的生命周期：各阶段怎么做安全，安全原则啊；

*做安全体系的各种模型：BLP、好多，就是做安全系统用的；

*模型的检测、评估和选优：TCSEC、CC、ISO15408 好多，有分功能和水平；

*通用硬件、软件的基本架构和安全功能、安全原理；

*实现安全的基本手段：密码学，反正不考数学和算法，不难，对称、非对称，散列什么 的，最重要的搞清密码学的应用，什么加密用在加解密、完整性、身份认证等什么场景，怎么用；

*怎么搞好一个站点的安全：设计、规划、建设和运维一个站点，各种物理安全要懂。

④通信与网络安全

*肯定先学网络架构和安全原则了：最重要的分层的思想，安全边界的运用，封装和解封的各层的协议。

*然后要清楚基本网络组件的安全：各种硬件设备啦、终端啦、介质啦；

*通信最重要的就是信道的安全了，最重要的方法就是 VPN 了，最重要的措施就是接入认证了；

*搞清楚各种针对网络的攻击和防御。

⑤身份与访问管理

*先是背景理论：什么是访问控制；

*访控的四个要素：好多要素，几个步骤；

*实现 4 个要素的身份管理系统：SSO 什么的；

*如何做好身份的标识和认证呢：单因素多因素什么的；

*授权机制：不同的需求和出发点用不同的授权；

*针对访问管理 IAM 的攻击和防御。

⑥安全评估与测试

安全好没好，只有搞了评估才知道。

*策略：目标、人员和责任；

*怎么做评估与测试,几个方面的工作：日志分析、代码测试、渗透测试，好多方法；

*收集了好多评估和测试的结果数据，就感知到企业的威胁了，安全态势出来了，安全措施必须要加强了；

*审计完了，审计报告怎么写呢？

⑦安全运营

*老外认为运维的第一重要工作合法合规，是要调查取证，不是为了保障业务。

*配置管理，这就是具体的运营工作了；

*运营的原则：可信路径、隐蔽通信什么的，好多；

*又讲一遍怎么具体的保护资产；

*运营的流程：事件的管理最重要。

*出了问题怎么办：

*怎么预防问题和事件：

*变更要管理，灾难要恢复；

*运营也包括对物理设施的运维，就是要保护好物理空间，都是物理的访问控制技术。

⑧软件开发安全

*软件开发的基础和安全原则，SDL，有数据库啊、语言啊什么的。基础内容很多，但不是直接出题的，题都在后面的内容里，放在具体场景里出；

*软件开发可能存在很多问题：漏洞、恶意代码、病毒；

*老美还很在意软件的评测和购买。

3.各域按出题比例排序（权重）：

01_安全与风险管理_Security and Risk Management_16%，40 题；

07_安全运营_Security Operations_16%，40 题；

05_身份识别与访问控制_Identity and Access Management_13%，33 题；

04_通信与网络安全_Communication and Network Security_12%，30 题

03_安全工程_Security Enginering12%，30 题；

06_安全评估与测试_Security Assessment and Testing_11%，27 题；

02_资产安全_Asset Security_10%，25 题；

08_软件开发安全_Software Development Security_10%，25 题。

共 250 道题。

第一域　安全与风险管理（例如安全、风险、合规、法律、法规、业务连续性）

Chapters 1,2,3,4,19 in OSG 7th

Chapters 2,9 in AIO 6th

A. 理解并应用保密性、完整性和可用性的概念

1. 安全的主要目的和目标就是 CIA 三要素/三元组

①机密性（Confidentiality）：机密性是指因为工作需要而访问敏感资源。机密性通常通过最小权限原则来实现。安全架构师使用数据分类、访问控制和加密来确保资源的机密性。

②完整性（Integrity ）：完整性包括两个方面，一是确保信息被正确处理且不被未授权的人修改，二是保护网络上传输的信息。完整性控制包括事务控制、数字签名等。

③可用性（Availability）：可用性确保资源可用、系统正常运行。可用性的防护措施多种多样，诸如集群、发电机、备份和热站等。影响可用性的威胁包括自然的、人为的灾难，还有拒绝服务攻击等。

这三个目标的对立面通常称为 DAD，即：破坏，篡改，和泄露。

这三个因素之间彼此影响。如：客体缺乏完整性，则机密性就无法被维护。又如：加密提供机密性，但如果密钥丢失，就会产生可用性问题。

不同机构对三元组的重要性排序也不同，如军队首先看重机密性，而企业更重视可用性。

2. 安全管理涉及的其它重要概念

在第五域还会复习这些概念。

①身份识别/标识（identification）ID

用户向系统声称其真实身份的方式。身份标识是一个过程，主体先表明或提供自己的身份，然后认证、授权，并且具备可问责性。计算机无法区分不同的人，只能通过 ID 账号来区别。（用户名是识别工具）

②身份认证（authentication）鉴别

测试并认证用户的身份。认证或检测所表明的身份是合法的过程，就是身份认证。最常见形式是使用密码。通过与合法身份(也就是用户账号)数据库中的一种或多种因素进行比较，身份认证能够识别并承认主体的身份。身份认证和上面的身份标识总是作为一个过程中的两个步骤被一起使用，不能分开。（密码、令牌都是认证工具）

③分配权限（authorization）授权

为用户分配并校验资源访问权限的过程。确保主体获得符合其身份级别的访问权限。（访问控制列表 ACL 是授权工具）

④可问责性/可追溯性（accounting）

确认系统中个人行为和活动的能力。只有在主体的活动可问责时，你才能够保持安全性。就是必须要检验主体的身份，并跟踪记录其活动。只通过密码认证是最不安全的，用户可能推卸自己的过失操作行为。

⑤不可否认性/抗抵赖性（undeniable）

能确认信息发送者即创建者的能力。不可否认性确保主体无法否认其已经发生的行为事件。不可否认性是可问责性不可缺少的部分，如果嫌疑人不承认有关证据或指控，那么他的行

为就无法被问责。

⑥AAA 服务（authentication、authorization、accounting）

就是指认证、授权和可问责，常用于身份认证系统，实际包括了五个方面的元素：识别、认证、授权、审计和可问责性。如果一个安全机制缺少这五个元素中的任何一个，则这个机制就是不完整的。

3.几种实现安全的解决机制（考题会问 XX 方法是利用和实现了什么安全机制？）

在操作系统里这些机制全都有应用，在第三域里要掌握，在第八域里也要掌握。

①分层

简单地使用、连续的多重控制，也被称为深层防御。比如物理上设置多道安检大门，技术上部署多套独立的不同原理的安防系统。“分层”和操作系统里的“环形”是差不多的。

②抽象

抽象有 2 种方式，一是面向对象编程，被抽象的对象组件内的操作和数据都是不可见的（黑箱）；二是将实体抽象分级，提高管理效率，比如：客体按密级分类，主体按职能分配角色等。

③数据隐藏

数据的物理存储空间是不能公开，也不能直接访问的，从而防止主体发现或访问数据。比如阻止应用程序直接访问硬件，不让未授权的访问者访问数据库等。

④加密

加密技术是安全控制非常重要，尤其在系统之间的传输数据时。

⑤进程隔离

进程隔离要求操作系统为每个进程的指令和数据提供不同的内存空间，并强制实施分界，以阻止某一进程读取或写入属于另外一个进程的数据。这样可以阻止未经授权的数据访问，也可以保护进程的完整性。

4.两种数据分级方案 classification

以前书上叫“分类”，以后用“分级”个词更准确。

一般公开的、非涉密的数据不列入分类级别，也不适用于“分级”这个专业术语。

①军政一般分三级

绝密(top secret)—秘密(secret)—机密(confidential)，和非机密(unclassified)。

这是教材的字面翻译，其实与中国实际不同，在国内军政是这么分的：

（核心）、绝密、机密、秘密、内部、公开。

②商业一般分三级（不同公司的标准不一样，CISSP 考的是这种标准）

机密(Confidential)——隐私(Private)——敏感(Sensitive)，以及公开(Pulbic)。

Confidential 是企业的，更高的是国家的 secret，最低的是个人的 Private。

B. 应用安全治理原则

什么是安全治理 secure governance？其实就是信息安全管理。

安全治理是与支持、定义和指导组织安全工作相关的实践集合。安全治理与企业治理和 IT 治理密切相关，其目标都是相同的，都是维持业务流程，同时努力追求增长和弹性。

安全治理是一个框架：即管理层提目标，实施层操作，共同实现企业安全的一个有效机制。

主要内容有：组织的安全目标、任务，组织级的流程，安全角色和职责，安全战略等等。（目标、责任、方法、检查）。第三方治理通常包括外部人员或审计人员，重点是外包服务的安全目标、要求、法规和合同义务的合规性。

常用的安全治理的实践标准有：ITIL、ISO27001、COSO、COBIT 等。

B.1 使安全功能与组织战略、目标和使命相一致 （例如：商业案例、预算和资源）

没什么要考的内容。

B.2 组织级过程 （例如：并购、剥离、治理委员会）

没什么要考的内容.

B.3 安全角色与职责

1.按照在安全环境中出现的逻辑顺序介绍六种安全角色：

在第二域 B 章节又把与处理数据相关的角色讲了一篇。

首先是信息安全官 CFO（Information Security Officer / Chief Security Officer），不解释了，分管安全的最高领导，还是要服从 CEO 的。

①高级管理者 Senior management

组织所有者(高层管理者)，负责所有策略、负有最终责任。所有活动在被执行之前，都必须得到高层管理者的认可和签字。

②安全专家/信息系统安全专家（Information systems security professionals）

安全专家、信息安全官或计算机应急响应团队(CIRT)，是受过培训和经验丰富的网络、系统和安全工程师，他们对落实高层管理部门下达的安全任务。主要包括制定和实现安全策略。安全专家不是决策制定者，他们只是实现者。

③数据所有者（Data owners）

负责对信息进行分级的人，是层次较高的、最终负责数据保护的管理者。不过实际管理数据的任务会委派给数据管理员来实施。数据所有者具有“应尽关注”的职责，要负责数据的分级，如果数据所有者工作繁忙，可以将数据保护的日常维护工作委托给数据管理员完成。

④数据管理员/保管员（Custodian）

负责实施安全策略和上层管理者下达的保护任务。包括：完成和测试数据备份、确认数据的完整性、部署安全解决方案以及根据分类管理数据存储。

⑤用户（user）

是具有安全系统访问权限的任何人。要求了解组织的安全策略，并遵守规定的操作过程，在已定义的安全参数内进行操作，以便维护安全策略。

⑥审计人员（Information systems auditor）

负责测试和认证安全策略是否被正确实现，以及相关的安全解决方案是否合适。审计人员要撰写合规情况报告和有效性报告，高层管理者会审查这些报告。负责检查系统，判断系统是否满足安全需求，以及安全控制是否有效

⑦安全委员会（security committee）

成员来自：高级管理层代表、IT 管理者、业务部门和职能部门负责人、信息安全官等。安全委员会的责任：决策并批准安全相关事务、策略、标准、指南和程序。

⑧安全管理员（Security Administrator）

负责实施、监视并执行安全规定和策略；各部门可以设立自己的安全管理员，负责执行本部门安全管理事务；向安全委员会/信息安全官报告。

⑨其它

帮助台（Help desk）：接报并确认安全事件，向合适的人员转达以便响应。

审计委员会（Audit Committee）：由董事会授权帮助检查和评估公司内部运行、内部系统审计以及财务报告的透明度和精确度以帮助相关利益人持续对公司有信心。

灾难恢复/应急计划人员：从整体上负责组织的应急计划；与应用所有者、信息安全人员等协同工作，取得其他应急计划支持。

应急响应团队 CIRT（Computer Incident Response Team）：评价安全事件和造成的损害，提供修补系统正确的响应，搜集证据。

搞清数据所有者、系统监管员、安全管理员的关系（必考）！

B.4 控制框架

安全规划步骤中最重要的一步，也是第一步，就是考虑组织想要的安全解决方案的整体控制框架或结构。而 CISSP 考试的一个重点构架就是**信息及相关技术控制目标**（COBIT），但不考它的详细内容，具体参考第九域中的法规。

1.3 种类型的控制：

①管理控制/软性控制（Administrative controls）。

②技术控制/逻辑控制（Technical controls）。是软件或硬件，例如防火墙、ID、加密、身份认证以及鉴别机制等。

③物理控制（physical controls）。保护基础设施、人身安全以及资源安全的物理设施。

2.常用的企业管控与治理的实践框架：

1.安全方案开发：ISO/IEC 27000 信息安全管理

2.企业架构开发：①Zachman, TOGAF 企业架构框架；②TOGAF；③DoDAF；④MODAF

3.安全企业架构开发：SABSA 安全架构框架

4.公司治理：COSO 企业内控管理模型

5.安全控制开发：①COBIT IT 内部控制；②NIST 800-53 安全控制参考

6.流程管理：①CMMI 软件开发管理；②ITIL IT 服务管理；③Six Sigma 业务流程管理

7.其他相关：①PMBOK, Prince2 项目管理；②ISO9000 质量管理；③ISO 38500 IT 治理；④ISO22301 业务连续性管理

这些不同的安全标准和框架不会考具体内容，但一定要清楚各自的目的和用途，会考某个情景应该选择哪种控制框架！（详见第九域）也要理解安全规划（宏观的安全管理）必须具有不断循环的生命周期，不断对其进行评估和改进。任何进程中的生命周期都可以用不同的方式描述，通常使用下面的步骤：

①计划和组织——②实现——③运营和维护——④监控和评估

3.与系统架构相关的概念定义

①架构 Architecture。就是一个客观存在的系统组织体系，包括系统的成员组成、相互

关系、设计原则等。

②架构描述 Architectural description (AD)。采用标准的表达方式描述架构组成的一系列文档。

③受益主体 Stakeholder Individual。其利益与该系统密切相关的团队、机构等。

④视图 View。从某些方面对整个系统的状况、态势进行展现。

⑤视角 Viewpoint。根据不同需要选择从哪些关注面去构建和使用一个视图。

B.5 尽职关注/应尽关注(Due Care)

①应尽关注/适度关注/应有义务/适度谨慎 Due care：就是通过合理的关注保护组织利益，例如：开发规范化的安全结构，包含安全策略、标准、基线、指导方针和程序等内容。

②应尽调查/应尽职责/应有责任/适度勤勉 Due Diligence：就是维持好应尽关注的成果。例如，将上述安全结构应用到组织的 IT 基础设施中。

企业要实现安全，就必须高度关注做好具体业务，还要高度重视做好审查分析。

讲了那么多，还是搞不清楚什么是关注，什么是调查，其实是先要做好了“调查”，才能做好“关注”。再换一种通俗的说法：

①**应尽关注 Due care（遵循规范/补漏洞）**：企业必须要承担这样的责任：尽心做好安全管理、尽力阻止安全漏洞、尽量消减安全风险，以减少潜在的利益损失和负面影响。举个例子：一家公司如果不花钱建立完善的防火措施，他就是没有履行“关注”的责任；当真的发生火灾了，股东、员工和客户都可以依法起诉这家公司，因为它没有履责而造成了重大损失。

②**尽职调查 Due Diligence（限定时间/找漏洞）**：企业必须要开展这样的活动：全面了解安全隐患、准确发现安全漏洞、客观评估安全风险，确保后续能真正有效地实施安全控制与保护工作。也就是说：公司必须经常分析潜在风险、发现火灾威胁，从而能及时提出要实施的防火措施。

B.6 尽职调查/应尽职责(Due Diligence)

写在上面了。

C. 合规

法律、法规相关的内容在第七域 B.4 章节也有。

合规性是符合或遵守规则、策略、法规、标准或要求的行为。

C.1 法律法规的合规

法律到底考什么，考多深，说不清楚，国际性的通用法规标准肯定会考到。这对所有应试者都是薄弱的章节，各种法案太多太乱了。不过再怎么样，也不会超出宝典里的内容，虽然很难记住。实际参加完考试，并没有回忆出太多太具体的直接考法规的题，尤其美国本土的法律原则上是不会考的，虽然各种练习题里有很多。

1.法律的类型

①民事法（民事准则）Civil law(code)：欧洲使用的，与美国的民事法律概念不同，下级法院不用服从上级法院。Rule-based law, not precedence-based。

②普通法 Common law：英国制定的，美、加、澳都用，包括刑法、民法（民事侵权）、行政（管理）法，使用法官和陪审团。Based on previous interpretations of laws。

③习惯法 Customary law：中国、印度等采用混合法律的地区使用，主要处理个人行为。Deals mainly with personal conduct and patterns of behavior。

④宗教法律体系 Religious law：伊斯兰国家使用，并不创建法律，而是试图发现法律的真理。Based on religious beliefs of the region。

⑤法例法律体系：通常由民法和普通法组成，荷兰、加拿大、南非等国用。

CISSP 考的是普通法法律体系（Common law），包括 3 类法：

①民法（侵权法）Civil law：处理针对个人或公司遭受的破坏或者损失，民事诉讼导致的结果是经济赔偿和或社区服务，而不是坐牢。如果有人在民事法庭状告另一人，陪审团会判断是谁的责任，而不是宣判有罪或者无罪。

②刑法 Criminal law：在一个人的行为违反政府法律时使用，是为了保护公众，判罚通常是坐牢。

③行政（管理）法 Administrative law：政府机构创建，用于监管公司或特定行业人员的表现和行为，如食品安全标准、防火规范等。

关于符合性(GRC)的概念

符合性通常指确保行为符合既定的规则以及提供工具来验证符合性的行为，它包括法律以及企业自身策略的符合性。

C.2 隐私要求的合规

详见 D.5 章节。

D. 在全球化背景下理解与信息安全相关的法律和法规问题

D.1 计算机犯罪

主要讨论美国的法律，CISSP 会考以下每个法律的目的是什么，主要内容是什么？（虽然原则上只考国际法规，但官方题库中涉及到了以下的所有法案）。

1. 计算机诈骗和滥用法案（Computer Fraud and Abuse Act）（历史第一个）

国会在 1984 年制定了计算机诈骗和滥用法案（CFAA），主要针对下列罪行：

①非法访问联邦系统中的机密信息或财务信息。

②非法访问联邦政府使用的计算机，以及联邦计算机进行欺诈活动

③对联邦计算机系统造成恶意损失超过 5000 美元的行为。

④非法修改计算机中的医疗记录。

⑤非法买卖计算机密码。

该法案在 1986 年进行了修正，主要拓展了使用范围，涵盖了：

①由美国政府专门使用的所有计算机。

②由金融机构专门使用的所有计算机。

③被用于进行犯罪的所有计算机组合。

2. 计算机安全法案（CSA 1987 年）Computer Security Act of 1987

国会还是不满 CFAA 的 1986 修正案，又制定了计算机安全法案(1987 年)，为所有的联邦

机构设置了安全要求基准。CSA 的四个主要目的是：

①明确由美国国家标准技术研究所(NIST)负责开发联邦计算机系统标准和准则，由美国国家安全局(NSA)提供技术性建议和援助。

②颁布并施行上述的标准和准则。

③要求所有使用涉密联邦计算机系统的操作人员，都要制定安全计划。

④所有相关的 管理、使用和操作人员强制性参加定期培训。

⑤它还指定了 NIST 负责公开系统的安防，NSA 负责机密级系统的安防。

这条法案的相关要求经过多年演进后，形成了联邦计算机安全策略的基础。

3. CFAA 修正案（1994 年）

1994 年，国会对上述法案又进行了大改。包括以下条款：

①生成任何类型恶意代码的行为是不合法的。

②法案适用于所有被用于州间贸易的计算机。

③允许关押罪犯，不管他们是否造成了实际的损坏。

④计算机犯罪的受害者可以提起民事诉讼，其受到的损失可以获得减轻和补偿。

2015 年，奥巴马也准备做个修改，把计算机犯罪纳入 RICO 条款范围中，即反诈骗腐败组织集团犯罪法(the Racketeer Influenced and Corrupt Organizations Act)，不知道现在正式颁布没有。

4.国家信息基础设施保护法案(1996 年)（National Information Infrastructure Protection Act of 1996）

1996 年，国会还是不满 CFAA，又通过了一系列修正案，再进一步扩展了其保护的范围，包括以下新覆盖的领域：

①放宽了法案的范围，除了用于州间贸易的计算机，还包括用于国际贸易的计算机系统。

②扩展了对国家基础设施(铁路、燃气、电力和通信线路等)的类似保护。

③故意造成国家基础设施重大损坏的行为，要从重处理。

5.联邦判决指导方针（Federal Sentencing Guidelines）

1991 年发布的联邦判决指导方针主要提供计算机犯罪的处罚指导、解释说明等，它最重要的三个条款是：

①提出**审慎者规则**（prudent man rule）。就是要谨慎工作，这种规则要求高管确保他能常态化的、持续的保持适度关注（due care）的态度；其它人员同样也要求保持谨慎工作的态度。这个规则以前用在在财政领域。（就是领导责任制）

②提出从轻处罚规则。对于有违法行为的组织机构和执行官，如果它能证明其保持并运用了适度关注的原则，并履行了自己的信息安全责任，那么可以从轻处罚。

③明确了要证明疏忽或差错确实成立的三个要素。即：被控人员必须具有法律上认可的责任；被控人员必须未遵守公认的标准；疏忽行为和后续损害之间必须存在因果关系。

④高管渎职可以处以最高 2 亿美元的罚款。

6.文书精简法案(1995 年)（Paperwork Reduction Act of 1995）

文书精简法案（199 年）要求组织机构必须获得美国行政管理和预算局 OMB(Office of Management and Budget) 的批准后，才能请求使用各类基础公共信息。2000 年的政府信息安

全改革法案 GISRA（The Government Information Security Reform Act）对它进行了修正。

7.政府信息安全改革法案(2000 年) GISRA （Government Information Security Reform Act of 2000）

国会要求 GISRA-2000 的拟制满足以下**五个基本目标：**

①要提供 1 个内容全面的体制。确保所有政府相关的信息资源安全、有效。

②要确保网络协同安全、有效。一切系统都是基于网络的，所以必须安全。

③要有效监控和掌握所有与安全风险相关的活动和信息。每个人的每个行为都要被监控。

④开发和维护联邦政府的信息安全防护系统。既要满足安全需求，也要实现最小成本。

⑤提供改进机制。能持续优化、完善联邦机构的信息安全监督体系。

GISRA 仍然明确，NIST 负责非机密系统，NSA 负责机密系统，并实行领导负责制。

GISRA 重新定义了计算机系统的分类，明确了**关键系统要满足以下条件：**

①被法律条款定义为国家安全系统。

②有机密信息且被相应的措施保护。

③系统被攻击会对机构的业务产生不良影响。

在这之后，国会总算不再折腾了，没有通过任何新的关于计算机犯罪的重大事项。虽然提了一些草案，都还没通过，如：2012 年的网络安全法案和 2013 年的网络情报共享和保护法案。

8.联邦信息安全管理法案 FISMA（Federal Information Security Management Act）

在 2002 年通过的联邦信息安全管理法案（FISMA），要求联邦政府实施一个信息安全项目，涵盖了政府部门的运营和外包商的活动。NIST 开发了 FISMA 的实施指南，提出了确保信息安全项目有效的关键要素：定期评估风险、安全意识培训、定期渗透测试、记录突发情况、制定应急响应流程等。

D.2 许可与知识产权（例如：版权、商标、数字版权管理）

世界知识产权组织(World Intellectual Property Organization,WIPO)简明地定义了知识产权。将知识产权分为两类：

①版权：涵盖了文学和艺术作品。**②工业产权**：如发明(专利)、工业设计和商标。

1.版权主要保护 8 类作品：

文学作品、音乐作品、戏剧作品、哑剧和舞蹈作品、绘画图形和雕刻作品、电影和其它音像作品、声音录音、建筑作品。

法律规定，只要创作者的作品产生出来，起就立即自动享有版权。如果能证明你就是作品的创作者，那么你就会受到版权法的保护。不过，在官方机构正式注册作品，可以政府承认他们在具体的日期收到了你的作品，并认可你的版权。越来越多的“盗版软件”(warez)站点出现了，这个 Warez 就是指非法传播盗版。

版权法不像商业秘密法那样保护特定的资源，它保护的是有资源意义的表达而不是资源本身。它保护表达方式，而不是其本身。

专利更多地针对发明本身，而版权则涉及如何再生产和分发。从这个角度看，对版权的保护弱于对专利的保护，但是版权保护的时间更长。版权的保护期是在受保护者的寿命基础上再加上 **70** 年。（死后再保护 70 年）

2.数字千禧年版权法案(DMCA)（Digital Millennium Copyright Act）

DMCA 中有 2 个条款（**打击盗版**）：

①阻止用户破坏版权保护机制。非法的复制会被处以巨额罚款。

②网络服务商（ISP）的线路被用于传播盗版，也要承担相应的责任。

3.商标（Trademarks）

商标是单词、口号和标志语，用于标识某家公司及其产品或服务。保护商标的主要目的是在保护个人和组织机构知识产权的时候避免市场的混乱。与版权的保护一样，为了获得法律的保护，商标不需要正式注册，可以使用 ™ 符号来表示出你想要保护作为商标的单词或口号。如果想让别人正式承认商标，那么可以在美国专利和商标局(US-PTO) 进行注册。注册的商标用 ® 符号表示。

在美国，商标准许的初始期是 10 年，可以再连续不受限制地使用 10 年（共 **20** 年）。

4.专利（Patents）

专利是最强的知识产权保护形式，保护发明者的知识产权，是授予个人或公司的法律所有权，使他们能够拒绝其他人使用或复制专利所指的发明。专利保护期一般是 **20** 年。

专利要满足以下要求：

①该发明必须是新的。（新）

①该发明必须是有用的。（有用）

③该发明不能是显而易见的。（难）

5.商业秘密（Trade Secrets）

商业秘密是公司特有的资产，对其生存和盈利有很大作用。版权和专利存在要公开细节，保护时限等问题，所有公司必须自己可是你办法保护商业秘密。很多公司都要求其员工签订一个保密协议 NDA(Non Disclosure Agreement)。

6.经济间谍法案(1996 年)(Economic Espionage Act of 1996)

经济间谍法案（1996 年）主要有 2 个规定：

①任何被发现为外国政府或机构而从美国公司窃取商业秘密的人，可以被处以高达 50 万美元的罚款和长达 15 年的监禁。

②任何被发现其它情况中窃取商业秘密的人，可以处以 25 万美元的罚款和 10 年的监禁。

7.许可证（Licensing）

要熟悉软件的许可证颁发协议。许可证有四种类型：

①签书面合同。②写在软件包装外面。③单击许可证协议来完善软件安装。④云服务许可协议，在屏幕上弹出一个确认已阅读并同意条款的确认框。

8.统一计算机信息处理法案 UCITA（Uniform Computer Information Transactions Act）

统一计算机信息处理法案(UCITA)，提供了计算机相关业务处理的共同架构，包括对软件许可证颁发的规定。UCITA 为上述的②、③形式的许可提供了法律描述和保护。还要求用户可以在安装之前拒绝许可证协议，生产商必须全额退款。它要求不同州之间的“许可协议”都符合统一的标准。

D.3 进口/出口控制

美国有两部法律与此相关：

①国际武器贸易条例法案(International Traffic in Arms Regulations Act，ITAR：1976)

②出口管理条例法案(Export Administration Regulations Act，EAR：1979)。

CISSP 考试要求对出口控制问题有大致的了解，是否有强加在科技和技术信息之上的限制和控制。

D.4 跨境数据流

瓦森纳协议(Wassenaar Arrangement)

WA 是对“常规武器和两用货品及技术”实施进出口管制的法律，来用阻止恐怖国家的军事实力增强，由 40 个国家共同制定了 9 类端口的出口规范，包括特殊材料、高科技设备、保密机等产品。

D.5 隐私

个人可识别信息 PII（Personally identifiable information）是用来唯一识别、联系或者定位一个人的数据，往往被用于身份盗窃、金融犯罪和各种犯罪活动中。

1.美国有关隐私的法律

好多，眼花缭乱。必考的，要背下来。

①第四修正案（Fourth Amendment of the Constitution）

隐私权的基础是美国宪法的第四修正案，内容如下：法律保护个人的人身、房屋、证件和财物不受无理的搜查和没收。搜查检索必须要有许可。

②隐私法案(1974 年)（Federal Privacy Act of 1974）

美国的隐私法案(1974 年)是对美国联邦政府有关公民个人私有信息处理的最重要的法律。任何机构在没有得到当事人书面同意的情况下，不得向他人泄漏隐私信息。

③电子通信隐私法案(1986 年)ECPA（Electronic Communications Privacy Act of 1986）

电子通信隐私法案(ECPA)规定对个人电子隐私的侵犯是犯罪行为。最重要的规定禁止窃听，不能偷电邮，否则处以最高达 500 美元的罚款和最高 5 年的监禁。（其实美国在窃听全世界）

④执法通信协助法案(1994 年)CALEA（Communications Assistance for Law Enforcement Act）

执法通信协助法案(CALEA)是对上面那个 1986 年的电子通信隐私法案的修正。它要求通信运营商允许持有法院命令的执法人员进行合法窃听。

⑤经济和专有信息保护法案(1996 年)EPPA（Economic and Protection of Proprietary information Act of 1996）

该法案将经济信息也视为财产，盗窃并不局限于物理产品。

⑥健康保险的易移植性和可问责性法案(1996 年)HIPAA（Health Insurance Portability and Accountability Act of 1996）

HIPPA 经常被考到，它要求医院、医师、保险公司和其它处理或存储个人医疗隐私信息的组织采取严格的安全措施，明确定义了个人在医疗记录方面的权利。

⑦2009 关于经济和临床健康的卫生信息技术法案 HITECH（Health Information Technology for Economic and Clinical Health Act of 2009）

关于经济和临床健康的卫生信息技术法案(HITECH)对 HIPAA 进行了修订。主要变化是针对商业伙伴(BAs)的。它将所有相关机构定义为：处理被保护的健康信息（PHI）的组织机构。任何 PHI 机构和一个商业伙伴（BA）之间的关系必须有书面合同管理，这个合同被称为业务联合协议（business associate agreement，BAA）。

HITECH 还明确了数据泄露的通告范围：发生泄密事件的 PHI 机构必须通知受影响的个人，影响超过 500 人时，必须通知卫生和人事服务部（the Secretary of Health and Human Services）的部长和媒体。

HITECH 是全国性的法律。此外，每个州都颁布了自己的相关法规。加利福尼亚州的 SB1386 是第一个发布的，涉及以下隐私信息：社会保险号、驾照号码、身份证号码、信用卡或借记卡号码、银行账户与安全代码、病历、医疗保险信息等。

⑧数据泄露通知法 DBNL（Data Breach Notification Laws）

若有泄密事件，当事单位必须在 60 天以内通知个人信息被非法访问。（如果影响超过 500 个人，还必须向媒体发布相关事件）。

⑨儿童联机隐私保护法案(1998 年)COPPA（Children’s Online Privacy Protection Act of 1998）

儿童联机隐私保护法案（COPPA）对儿童网站的信息保护提出了一系列要求。它要求任务组织必须要取得父母的同意后，才能收集 13 岁以下儿童的信息。

⑩Gramm-leach-Bliley 法案(1999 年) GLBA/金融服务现代化法案/格蕾姆

GLBA-1999，严格限制了银行、保险公司等商业机构之间的信息共享和服务提供。

⑪美国爱国者法案(2001 年)（USA PATRIOT Act of 2001）

这个是国会对 2001 年 911 事件的响应。它扩大情报机构的权限，将以前一次只能获取一条线路的监听授权扩大为可以获得对一个人的有所通信进行监听的一揽子授权。另一方面，允许网络服务提供商(ISPs)提供更多的信息。它 OpenID 还修正了计算机欺诈和滥用法案(CFAA)，对犯罪行为从重处理。

⑫子女教育权利和隐私法案 FERPA（Family Educational Rights and Privacy Act）

FERPA 是关于教育机构的，保护成年学生和未成年学生父母的隐私权。

⑬身份偷窃和冒用阻止法案(1998 年)（Identity Theft and Assumption Deterrence Act）

就是规定身份偷窃是严重的犯罪行为。

⑭萨班斯-奥克斯利法案(SOX-2002) Sarbanes-Oxley ACT

2002 年的该法案(简称为 SOX)适用于在美国上市的任何公司，其中的许多法律被用于监管会计行为以及公司上报财务状况所使用的方法。然而，某些部分(特别是 404 条款)直接适用于信息技术。SOX 对公司如何追踪、管理和报告财务信息提出了专门要求，这包括保护财务数据并保证它的完整性与真实性。大多数公司都依赖计算机设备和电子存储来进行事务处理和数据归档，因此公司必须采用适当的流程和控制来保护这些数据。公司管理人员，包括首席执行官(CEO)、首席财务官(CFO)和其他人员，如果不遵守 Sarbanes-Oxley 法案，那么可能导致严厉的处罚，甚至可能会入狱数年。

2.欧盟有关隐私的法律

①概括指令（directive outlining privacy measures）

1995年，欧盟(EU)议会也通过了描述隐私措施的概括指令（directive outlining privacy measures）。要求所有个人数据的处理要满足有关标准，明确了个人对自己信息的处理权利。

②美国—欧盟安全港湾项目/安全避难所（避风港 Safe Harbor program）

经过与联邦数据保护和信息、委员会的商讨，美国商务部开发了独立的安全港湾框架来调和欧美对于隐私不同的处理方式，并给美国组织提供一种优化的方法以符合欧盟数据保护法的要求：数据出口方和进口方之间的合同必须需要事先获得国家数据保护当局的批准，方可传输数据到国外。为了符合安全避难所规定，在欧洲进行商业活动的美国公司必须满足7项处理个人信息的要求。这里强调下经常考的7个安全港原则。这是美国贸易部的一个控制机制，防止未授权的信息泄露，相关的术语有：

1)通知 notice：任何组织必须告知个人使用数据的目的。（告知我）

2)选择 Choice：任何组织必须为个人提供可选择的机会。（我选择）

3)向前传输 Onward transfer：组织只有在遵守通知及选择规则的基础上才能向其他组织传输资料。（别乱传）

4)安全 Security：组织必须保护好数据。（别泄密）

5)数据完整 Data integrity：组织不得将信息挪用，还要确保数据真实可信。（别乱改）

6)访问 Access：个人可以查、改或删组织所持有的他们的个人信息。（属于我）

7)执行 Enforcement：组织必须落实以上各条原则。（别搞事）

安全港湾项目的目的是有效衔接美国与欧盟不同的隐私法律与标准，主要针对的是欧盟的The EU Data Protection Directive（欧联数据保护纲领），它就包括了上面的7个原则，不过它也将在2018年被GDPR (European Union’s General Data Protection Regulation)取代。

3.支付卡行业数据安全标准（Payment Card Industry Data Security Standard）

支付卡行业数据安全标准(PCI-DSS) 是一个非法律但有合同义务的优秀合规要求典范。有12个主要要求，不列举了。它提供了一系列关于支付安全控制的标准。

D.6 数据泄露/数据破坏

了解下法规，基本上就是出现泄密事件必须24小时内上报。

1.电子通信服务规范(Regulation for Electronic Communication Service, EU: 2013)

欧洲电子通信服务提供者，需要在检测到个人数据泄露后不迟于**24小时**向国家主管当局提供个人数据泄露的数据泄露通知。

2.隐私和电子通信法规(Privacy and Electronic Communications Regulations.UK: 2013)

电子通信服务提供商，诸如电信，互联网服务供应商(ISPs)，在知道数据泄露的基本事实后必须在**24小时**内通知UK信息专员办公室。

E. 理解职业道德

E.1 践行(ISC)² 职业道德规范 Code of Ethics

在你参加考试和成为 CISSP 之前会被要求签署(ISC)²道德规范。你需要理解道德规范并把它应用到现实当中，诸如组织内的用户群体的道德责任。

1.(ISC)2 道德规范序文 Code of Ethics Preamble

The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

“我们坚守国家安全，对雇主负责，始终遵守最高的道德行为标准和相关要求。”

“因此，严格遵守这些准则是通过认证考试的必然条件。”

2.(ISC)2 道德规范准则 4 条/Code of Ethics Canons:

*Protect society, the common good, necessary public trust and confidence, and the infrastructure.

*Act honorably, honestly, justly, responsibly, and legally.

*Provide diligent and competent service to principles.

*Advance and protect the profession.

①保护社会，国家和基础设施。

②行为诚实、正直、公正、负责和合法。

③为雇主尽职尽责服务。

④提升能力和促进行业发展。

顺序很重要，①是最重要的准则。

3.尊重考试

A CISSP candidate and a CISSP holder should never discuss with others what was on the exam. This degrades the usefulness of the exam to be used as a tool to test someone’s true security knowledge. If this type of activity is uncovered, the person could be stripped of their CISSP certification because this would violate the terms of the NDA upon which the candidate enters prior to taking the test. Violating an NDA is a violation of the ethics canon that requires CISSPs to act honorably, honestly, justly, responsibly and legally.

已经通过 CISSP 考试的人不得与其它任何人谈论、议论或讲授关于考试内容的信息，针对应试而进行的真题收集等活动，将严重影响考试对考生真实能力素质的评估效果，从而大幅降低这项测试信息安全从业人员真实知识水平的，客观、准确、公平的认证考试的含金量和可靠度。有此类违规行为的 CISSP 人员，既违反了考试的保密协议，也违反了 CISSP 的职业道德，将吊销其证书。请不要尝试收集真题，保持其应有的考试难度，控制通过比例。

E.2 支持组织的道德准则

1.四类道德标准

①全球责任；②国家；③组织；④个人。

2.计算机道德协会(Computer Ethics Institute)

是一个非盈利组织，它以道德的方式帮助推进技术发展。制定了它自己的计算机道德 10 诫(Ten Commandments of Computer Ethics)：

(1)不得使用计算机伤害其他人。

(2)不得干预其他人的计算机工作。

(3)不得窥探其他人的计算机文件。

(4)不得使用计算机进行盗窃。

(5)不得使用计算机提交伪证。

(6)不得复制或使用尚未付款的专利软件。

(7)在未获授权或未提交适当赔偿的前提下，不得使用其他人的计算机资源。

(8)不得盗用其他人的知识成果。

(9)应该考虑你所编写的程序或正在设计的系统的社会后果。

(10)在使用计算机时，应考虑尊重人类。

3.互联网架构研究委员会(Internet Architecture Board, IAB)

IAB 是用于 Internet 设计、工程和管理的协调委员会。它负责对 Internet 工程任务组(Internet Engineering Task Force, IETF)的活动、Internet 标准流程(Internet Standards Process)的监督和上诉、注释请求(Request for Comment, RFC)的编辑进行架构监督。否则，Internet 将无法正常使用。

F.制定并实施文档化的安全策略、标准、程序和方针

以下描述的内容都是规范化的安全策略结构中的几大要素，搞清楚是什么：

1.安全策略(Security Policies)

规范化的最高层次被称为安全策略。安全策略是一个文档，包括：组织的安全需求、安全目标、安全原则、安全架构，定义所有相关的术语，定义角色、分配职责，指定审计要求等等。

安全策略是强制性的，包括特定问题的安全策略、特定系统的安全策略和综合的安全策略类，综合的安全策略有 3 种类型，包括：规章式的、建议式的和信息式的。

①**规章**式的策略（regulatory policy），主要涉及必须遵守的行业标准或法律规定；

②**建议**式的策略（advisory policy），解释了高层管理对内部安全和合性性的期望，包括可接受的行为和活动，并定义违背安全性的后果。大多数安全策略都是建议性的。

③**信息**式的策略（lnformative policy），提供了与相关的支持、研究或背景信息，用于提供特定的信息或知识，例如公司目标、任务声明或者组织如何与合作伙伴和客户进行交流。

根据内容策略分为 3 种类型：

①组织性策略（Organizational or program policy）：此类策略由高级管理层发布，该策略描述并委派信息安全责任，定义实现 CIA 的目标，强调需要特别关注的信息安全问题（例如保护信用卡公司或健康保险公司的机密信息，或者高可用性系统）。通常情况下，此类策略的范围是整个组织。

②功能型策略/特定问题策略（issue-specific policy）：针对特定安全领域或关注点，例如访问控制、持续性计划、职责分离等，或者针对特定的技术领域，例如使用互联网、电子邮件、无线访问、远程访问等。此类策略依赖于业务需要和可接受的风险水平。内容包括：对特定问题的阐述，组织针对该问题的态度，适用范围，符合性要求，惩戒措施等。

③特定系统策略（System-specific policy）：针对特定的技术或操作领域制定的更细节化的策略，比如特定应用或平台。

2.策略链

策略是层次性的，下面是至上到下的策略链：

方针(最高策略)=>标准(技术方法)=>基线(最低标准)=>指南(运用标准)=>程序(操作实现)

它们的关系：安全策略是有组织的安全文档的总体结构的基础；然后，标准基于策略并受规章制度的管辖；指南从其中衍生而来；最后，程序基于前面三个基本要素。

①策略/方针 Policy：处于策略链的最高层次，它是由组织的高级管理层发布的、关于信息安全最一般性的声明。方针应该代表着高级管理层对信息安全承担责任的一种承诺，一旦发布，要求组织成员必须遵守。**策略**/方针的实施要依靠标准、指南和程序。

②标准 Standard：标准规定了在组织范围内强制执行的对特定技术和方法的使用。标准起着驱动方针的作用，标准可以用来建立方针执行的强制机制。

③基线 Baseline：基线建立的是满足方针要求的最低级别的安全需要。在建立信息安全整体框架之前，基线是需要考虑的最低标准。标准的开发通常都是以基线为基础的，基线可以看作是抽象的简单化的标准。大多数基线都是很具体的，或者与系统相关，或陈述某种配置。基准往往指的是行业或政府标准，例如可信任计算机系统评估标准(TCSEC)或信息技术安全评估和标准(ITSEC)或者 NIST(美国国家标准技术研究院)标准。

④指南 Guideline：类似于标准，也是关于加强系统安全的方法，但它是建议性的。指南比标准更灵活，考虑到了不同信息系统的特点。指南也可用来规定标准的的开发方式，或者保证对一般性安全原则的遵守。作为安全专家和用户的操作指南，提供了如何实现标准和基准的建议。指南说明了应当部署哪些安全机制，概述了一套方法(包括行动建议)，但并非强制性的。彩虹系列、通用准则 CC、BS7799 等，都可以看作是此类。

⑤安全程序/过程/措施/实施 Procedure：是执行特定任务的详细步骤。位于策略链的最低层次，是实现方针、标准和指南的详细步骤。安全程序是详细的、按部就班的指导文档，它描述了实现特定安全机制、控制或解决方案所需的确切行动。

G.理解业务连续性要求

本章必考

1.业务连续性计划（BCP）和灾难恢复计划（DRP）之间的差异。

①BCP 是预防性的、全面、持续的，必须被首先应用（实施），并持续的应用。

②DRP 是补救性的、应急、临时的，当 BCP 失败了(leaves off)，就会启动 DRP(picks up)。

灾难恢复 DRP 的目的是，尽量减少灾难或中断所带来的影响，尽可能快的恢复正常的业务活动。DRP 只在灾难发生后才实施。灾难恢复处理“我的天哪，天要塌了”，而连续性规划处理“好了，天塌下来了。现在，我们该如何继续经营?

虽然文字上都写的是“计划-PLAN”，但实际上它不只是一系列的文档方案，还包括了相关的应对工作、实施过程和实践操作。

考试中的灾难恢复 DR，是指对技术环境的恢复，是以信息技术为核心的，也就是信息系统的恢复，而不是对整个组织管理、业务运行、物理环境、生产能力的恢复。

业务连续性管理（BCM），是整体的管理过程，包含 DRP 和 BCP，提供一个框架，实施管理，形成能力。BCM 的主要目的是允许该组织继续在不同条件下进行业务操作。

2.业务连续性计划（BCP）的步骤

ISC² 定义的创建业务连续性计划的过程包括以下四个主要步骤：

①编制计划；②评估业务影响；③连续性计划；④批准和实现。

在第七域的 N 章节，详述了 NIST 800-34 规范的业务连续性管理的流程，和上面的不一样。

考题里问 BCP 的第一个步骤，一般选业务影响分析 BIA（包括分析关键业务、调研各个部门），而不是计划。

G.1 制定并记录项目范围和计划

业务连续性计划 BCP 的步骤流程就是下面的 1、2、3、4 步，其中的“企业组织架构分析”要做 2 次！BCP 第一步：先一个人来做企业组织架构分析；然后他牵头组建 BCP 团队；接着 BCP 团队再做一次企业组织架构分析，来修订和验证之前他做的分析；之后才获取资源干正事了。

1.先分析企业组织架构（业务组织分析）Business organization analysis

分析组织架构是重要的基础工作，为确定 BCP 团队成员提供了根据，通常由 BCP 先头部队来完成。需要考虑的关键部门有：核心业务运营部门、支撑保障部门（IT、维修等）、高管人员等。

2.再选择 BCP 团队 BCP team selection

团队要包括各种各样的关键人物，团队领导一定要是企业的高管之一，才好有效落实。

2.5 再做一次全面的企业组织架构分析。

3.再获得相关资源 resource consumed

不同阶段要有不同的资源来支撑保障 BCP 有效实施。

①BCP 开发：前面提到的四个步骤(项目范围和计划编制、业务影响评估、连续性计划、批准和实现)，最需要的资源就是人力，也就是抽组人员、集中办公、拟制计划。

②BCP 测试、培训和维护：这时候要有基础环境的保障，也就是软、硬件设施。当然，人力总是不可缺少的。

③BCP 实现：当灾难和意外发生时，更就需要大量的资源来执行 BCP，反正什么都要。

4.还要考虑法律、法规要求（合规）Legal and regulatory assessment

在业务连续性计划实施过程中，聘请法律顾问是非常重要的。

5.安全管理计划小组应该开发三类计划：

①战略计划（strategic plan）是长期计划（例如 5 年），相对稳定，定义了组织的目标和使命。

②战术计划（tactical plan）是中期计划（例如 1 年），是对实现战略计划中既定目标的任务和进度的细节描述，例如维护计划、系统开发计划、变更管理、技术革新、容灾备份等。

③操作计划（operational plan）是短期的高度细化的计划，须经常更新（每月或每季度），例如培训计划、系统部署计划、产品设计计划等。

G.2 开展业务影响分析

BCP 团队完成了准备创建业务连续性计划的四个阶段，就会进入工作的核心部分：**业务影响分析/评估(BIA)**。BIA 先确定决定组织持续发展的资源，再分析资源的潜在威胁，再评估每种威胁的可能性和对业务的影响。BIA 的定量分析、定性分析在第一域 I.2 章节里讲过了。（相关内容在第六域 C.6 章节和第七域 N 章节里面也有涉及）。

BIA 的标准流程是 4 步：

①收集信息。Gathering information。识别和列举组织的所有业务。

②评估脆弱性。Performing a vulnerability assessment。

③分析业务影响。Analyzing the information。

④拟制并呈报分析报告。Documenting the results and presenting the recommendations。

1.确定业务优先级

BIA 的第一个任务是确定业务优先级，就是当灾难发生时，哪个业务最重要，最先被恢复。

这里涉及几个常用概念：

①最大允许中断时间（MTD）Maximum Tolerable Degradation，也称为最大容忍中断时间（MTO），指的是某个业务功能出现故障但是不会对业务产生无法弥补的损害所允许的最大时间长度（底线）。

②恢复时间目标（RTO）recovery time objective，就是当中断事件发生时，实际恢复功能的时间期望。

BCP 过程的目标是确保你的 RTOs 小于 MTDs。

很明显，MTD 最短的业务，其优先级就越高！

2.识别风险

识别风险是一个纯粹的定性分析的过程，就是列出可能的各种风险。自然或人为的风险。

3.业务影响评估

这里要考虑到所谓的云服务的可靠性，当企业的某个服务外包给第三方公司时，它的中断风险一定要考虑到。

4.可能性评估

就是要算出年发生比率(ARO)。

5.影响评估

这里要定义暴露因子 EF，计算单损 SLE，计算年损 ALE。当然，也可以用定性的方法，只评级，不量化计算。

6.资源优先级划分 Resource prioritization

BIA 的最后一个步骤，因是针对各种不同风险，确定分配业务连续性资源的优先级。如果生成了一个所有风险的列表，那么年损最大的风险优先级就最高。

前面只是做了影响分析，下面要开始写 BCP 计划了

7.策略开发 strategy development

BCP 团队现在根据风险优先级列表，确定采取什么应对措施（减轻、转移、接受和拒绝）。这是衔接业务影响分析 BIA 和业务连续计划拟制工作的环节！这个策略的主要内容包括:范围、任务说明、原则、指南和标准。

8.预备和处理 Provisions and processes

有了 BCP 策略，就要研究怎么保护人、建筑物与设备、基础设施等，采取什么措施缓解（mitigate）不可按受的风险。这里就要研究实际的风险消减机制、方法、手段了。

9.计划批准

一旦 BCP 团队完成了 BCP 文档的设计，那么就该呈上审批了。高层的决策是最关键的。

10.计划实现

计划被批准了，就要落实了，包括资源分配、计划维护什么的。

11.培训和教育

培训和教育是落实 BCP 计划的一项重要内容，确保人员在灾难发生时能够有效地完成其任务，人员还要有所冗余。

12. BCP 文档化

成体系的，持续的修订、完善和保存 BCP 文档，确保该项工作有序开展。

现在算是完成业务连续性的计划的研究拟制和预备实施工作了，有些具体的执行和维护工作在第七域的灾难恢复里讲。

H.促进人员安全策略

雇用新的职员涉及几个明确的步骤：①创建工作描述、②设置工作分类、③筛选候选人、④雇用和培训最适合这项工作的人。

1.员工管理方面的重要元素包括责任分离、工作职责和岗位轮换

①职责分离（Separation of Duties）

职责分离属于安全概念，是指把关键的、重要的和敏感的工作任务分配给若干不同的管理员或高级执行者，是将最小权限原则应用到管理员身上。这样做能避免一个人能够独自干成一件坏事，也能防止共谋 collusion。共谋指的是几个人的团伙一起干成一件坏事。

②工作职责（Job Responsibilities）

工作职责是要求员工在常规的基础上执行特定工作任务。这个概念主要用来确定员工的最小访问权限。

③岗位轮换（Job Rotation）

让员工在不同的工作岗位中轮换职位，从而提高整体的安全性。岗位轮换有两种功能：一是提供知识和人员的冗余，缺谁都照样运转；二是提供了一种同级审计形式，减少伪造、篡改、偷窃、破坏和信息滥用的风险，也能够防止共谋。

④交叉训练（Cross-training）

是工作轮换的另一种形式，员工不换岗位，只是跟班学习或者临时顶替一下，是一种应急预案。

上面的①、②、③都是经常考的。

H.1 求职人员甄选 （例如：证明人核实、教育背景查证）

要确保任职人员的安全性，必须做背景调查和安全检查。

背景调查

背景调查包括：获得候选人的工作和教育历史记录，检查证明材料，与候选人的同事、邻居和朋友进行面谈，向警察局和政府机关调查候选人的拘捕或违法活动记录，通过指纹、驾驶执照和出生证明来认证身份，还要进行面试。如有必要，也可以采用测谎仪、药检、性格测试/评估等形式。很多公司还要对申请人进行在线背景调查和社交网络账号复审。

重要的安全岗位对人的道德素养要求很高，所以别用自己的身份证去乱开房，还有手机号、银行账户都会被查的。

H.2 雇佣协议与政策

新员工入职，要签署雇佣协议和保密协议。

1. 雇佣协议

协议文档说明了组织的规则和限制、安全策略、可接受的使用和行为准则、详细的工作描述、破坏活动及其后果、要求员工胜任工作所需的时间。

2. 保密协议（NDA）

NDA 用来保护组织的机密信息不会被的员工泄漏。

3. 竞业禁止协议（NCA）

NCA 通常与 NDA 同时存在。NCA（竞业禁止协议）防止了解公司核心秘密的员工进入另一个存在竞争关系的组织机构，也能防止员工因为高薪而跳槽到另外的公司。通常，NCA 具有时间限制，例如半年、一年甚至三年。

强制执行 NCA 是有一定困难的，法律上认可员工为了保障自己和家庭的生活，允许使用所具备的技能和知识谋取工作，NCA 不能妨碍员工获得适当的收入。但是它的威慑作用和保密作用还是明显的。

4. 强制休假

强制员工休假，可以提供与岗位轮换类似的好处。代班的人员可以审计发现他的过失。

H.3 劳动合同解除流程

解雇 1 个员工时，应该：

①采取不公开的和尊重人的方式。

②终止合同时应该至少有一位证人在场，证人最好是高层经理或保安人员。

③一旦员工被告知离职，应该被立刻护送离开，并且不允许通过任何理由返回办公地点。

④在员工被解雇离开之前，所有组织特有的身份证件、访问权限或员工安全标志以及门卡、钥匙和出入证都应该被收回。还必须在通知员工被解雇的同时或之前，就禁止或删除此员工对系统的访问权限。

解雇员工的最佳时间是员工轮班结束的时候。一方面，留给时间去寻找新的就业机会；另一方面，换班时解雇更加自然，可以减少压力。解雇员工时，根据员工的心理状态，视情进行一次离职面谈，目的是：根据之前签署的雇用协议和保密协议来审查其责任和约束条件。

H.4 供应商、顾问与承包商的控制

在使用任何类型的第三方服务提供商时，服务级别协议(SLA)尤为重要。

H.5 合规

详见 C 章节。

H.6 隐私

隐私性的定义多种多样，大概意思就是：

①防止对个人重要信息的未授权访问。

②防止未被同意或知晓情况下，检查、监控其行为。

个人身份信息（PII）personally identifiable information

PII 是可以追溯到源头的人的任何数据项。如：一个电话号码、电子邮件地址、邮寄地址、社会保障号、名字、信用卡账号、银行账号等；没有代表性的个人信息不是 PII，如：一个 MAC 地址、IP 地址、操作系统类型、最喜欢的度假地点、高中吉祥物的名字等等。

I. 理解与应用风险管理的概念

理解风险管理的概念是 CISSP 考试的重点（必考）。

风险管理的主要目的是要将风险降低到一个可以接受的级别。达到风险管理主要目标的过程被称为风险分析（risk analysis）。风险评估（Risk Assessment）是对信息资产及其价值、面临的威胁、存在的弱点，以及三者综合作用而带来风险的大小或水平的评估。

信息风险管理 IRM (lnfonnation Risk Management)是识别并评估风险、将风险降低至可接受级别、执行适当机制来维护这种级别的过程。

风险分析提供了一种成本/收益比(costl-benefit comparison)，也就是用来保护公司免受威胁的防护措施的费用与预料中的损失所需要付出的代价之间的比值。在大多数情况下，如果损失的代价没有超过防护措施本身的费用，那么就不应该实行该防护措施。风险分析有下列 4 个主要目标：

①标识资产和它们对于组织机构的价值。

②识别脆弱性和威胁。

③量化潜在威胁的可能性及其对业务的影响。

④在威胁的影响和对策的成本之间达到预算的平衡。

1. 重要术语

我们常常使用术语“脆弱性”、“威胁”、“风险”和“暴露”来表示同样的事情，然而，它们实际上有不同的含义，相互之间也有不同的关系。理解每一个术语的定义是非常重要的，但更重要的是应当理解它们彼此之间的关系。

①资产（Asset）

资产是指环境中应该加以保护的任何事物。如：计算机文件、网络服务、系统资源、进程、程序、产品、IT 基础架构、数据库、硬件设备、家具、产品秘方/配方、人员、软件和设施等。。

②资产估值（Asset Valuation）AV

就是资产具备的货币价值。包括开发、维护、管理、宣传、支持、维修和替换资产的所有

成本，还包括公众信心、行业支持、生产率增加、知识资产以及所有者权益等无形价值。

③弱点/脆弱性（Vulnerability）

一个资产的弱点（缺少安全措施）、缺陷（安全方面的问题）或者漏洞被称为脆弱性。一旦被利用，就会对资产造成损害。如果没被利用，当然也就没事了。

③威胁（Threats）

前面讲了脆弱性，那么一个弱点有多个大可能会被利用，并产生破坏呢？

威胁就是利用脆弱性的行为，它会带来危险：即某人或某个软件识别出特定的脆弱性，并利用其来危害公司或个人。任何可能发生的、造成资产价值损失的事情都被称为威胁。威胁主体通常是人，不过也可能是程序、硬件或系统。威胁事件包括火灾、地震、水灾、系统故障和人为错误(一般是因为缺少培训或无知)和断电等等。

⑤风险（Risk）

脆弱性、威胁都是客观可能存在的东西或者事件，而风险就是一个量化的指标（百分比或者经济损失的价值），代表了是某种威胁事件利用了脆弱性，并导致资产损害的可能性。它是1个概率性的评估。可能性越大，风险就越大，损失就越大。

风险=（威胁+脆弱性）×100%=潜在影响

会考到风险相关的三要素：威胁、脆弱性和消减措施。

⑥暴露（Exposure）

显示脆弱性，把组织暴露在威胁之下。暴露就是存在可利用的脆弱性。暴露并不是指威胁事件实际发生了，而是存在漏洞被利用的潜在可能性，或者是资产被迫害的可能性。也就是说，没暴露前，没人知道系统有脆弱性、威胁和风险，一切都是安全的；只有真实暴露了，才会发生实际的安全事件，一切才变得不安全。

⑦防护措施（Safeguards）

防护措施就是安防对策，是指能消除脆弱性或应对一种或多种特定威胁的任何方法，包括技术的、物理的、管理的。当然，一切的目的是为了消减风险（mitigate risk），包括控制(control)、对策（countmeasure）和防护措施（safeguard）。

⑧攻击（Attack）

攻击是1个威胁主体利用脆弱性的行为，前面几个概念都是纸上谈兵，只有攻击发生了，才产生实际的、真正的破坏性影响。搞攻击就是搞破坏，搞破坏就是

⑨破坏（Breach）

破坏就是破解了或者绕过了安防系统，也就是实现了非法进入。搞成了破坏，就能搞攻击了。当破坏与攻击结合时，就会发生渗透事件或入侵事件。

⑩残留风险（Residual Risk）

在实施安全措施之后仍然存在的风险。

最后用一个图来描述关系：

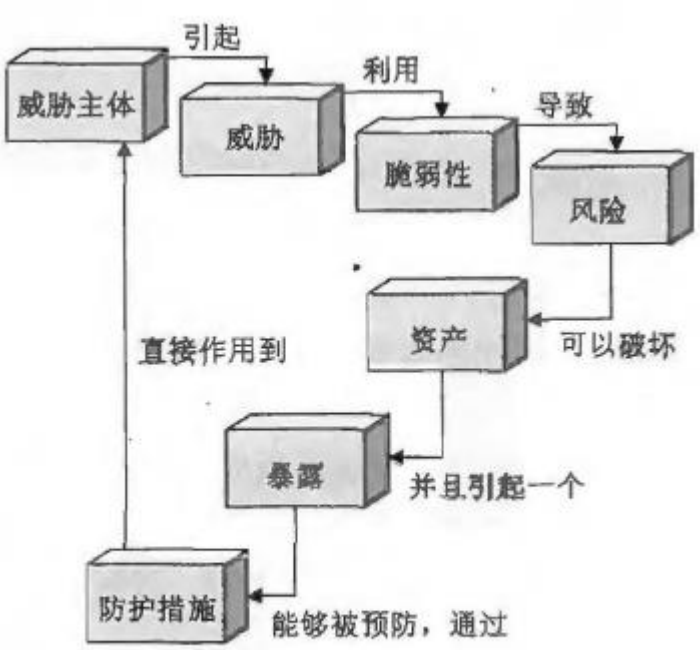


图 2-2　各种安全组件之间的关系

表 2-5　威胁和脆弱性之间的关系

威 胁 主 体	可能利用的脆弱性	导致的风险
恶意软件	缺少防病毒软件	病毒感染
黑客	服务器上运行的功能强大的服务	对机密信息的未授权访问
用户	操作系统中配置错误的参数	系统故障
火灾	缺少灭火器材	设施和计算机受到破坏，可能付出生命代价
雇员	缺少训练或实施标准 缺少审计	共享至关重要的信息 在数据处理应用程序中更改输入和输出
承包商	松懈的访问控制机制	窃取商业秘密
攻击者	编写较差的应用程序 缺少严格的防火墙设置	造成缓冲区溢出 进行拒绝服务攻击
入侵者	缺少保安	打破窗户，盗窃计算机和设备

2. 美国 NIST 的风险评估过程

NIST 开发了一套风险方法，出版在 SP 800-30 文档中。这套 NIST 方法叫做信息技术体系风险管理指南(Risk Management Guide for Information Technology System)，被认为是美国联邦政府标准。

①准备评估。

目标是搞清背景。

*确定评估的目的，*确定评估范围，*识别与评估有关的假定与约束，*识别评估的输入，*识别评估期间使用的风险模型和分析方法。

②进行评估。

目标是生成信息安全风险列表，从而根据风险水平区分优先级，并通知风险响应决策。

*识别与组织相关的威胁源，识别这些源可能产生的威胁事件，

*识别组织内可被威胁源利用的脆弱性，

*确定威胁源会引发的特定威胁事件的可能性，以及威胁事件成功的可能性，

*确定威胁事件产生的负面影响

*确定威胁负面影响的信息安全风险。

③沟通评估结果和分享风险的相关信息。

目的是确保决策者了解掌握风险相关的信息，指导风险决策沟通，共享信息。

*沟通风险评估结果，*在风险评估的执行阶段共享相关信息，支持其他的风险管理活动

④维护评估。

目的是跟踪掌握风险变化情况。

*监控风险评估中识别的风险因素，掌握后续变化，*更新风险评估报告。

3.ISO/IEC 27005

一个国际标准，规定在 ISMS 框架内如何进行风险管理。

I.1 识别威胁与脆弱性

对 IT 的威胁并不只限制在 IT 源，也有自然灾害、人和管理的因素。脆弱性评估需要一个技术团队，也需要非专业的人员来提高全面性。

通过常使用微软的 STRIDE 威胁分类方案（6 个首字母）。即：

①电子欺骗(Spoofing)——通过使用伪造身份获得对目标系统访问权限的攻击行为。可使用 IP 地址、MAC 地址、用户名、系统名称、无线网络名称、电子邮件地址以及许多其它类型的逻辑标识来欺骗。

②篡改(Tampering)——任何对数据进行未授权的更改或操纵的行为，包括在传输中的和被存储的数据。这种攻击主要侵害完整性和可用性。

③否认(Repudiation)——用户或攻击者否认执行了一个动作或行为的能力。也就是抵赖、不承认有过非法行为。

④信息披露(Information disclosure)——将私人、机密或受控信息揭露、传播给外部或未授权实体的行为。

⑤拒绝服务(DOS)——指攻击试图阻止对资源的授权使用。这可以通过缺陷开发、连接重载或流量泛滥实现。DOS 攻击并不一定会导致对一个资源的完全中断；而是会减少吞吐量或造成延迟，以阻碍对资源的有效利用。

⑥权限提升(Elevation of privilege)——此攻击是指有限的用户帐号被转换成一个拥有更大特权、权力和访问权的帐户。

一骗二改三抵赖；窃密瘫痪提权限。

I.2 风险评估/分析 （定性分析、定量分析、混合分析）

要搞清 2 种风险分析的区别：

①项目风险分析 project risk analysis：团队针对项目实施的分析，为了避免项目失败。

②安全风险分析 security risk analysis：仅针对某个信息系统的分析，为了找其漏洞。

1.风险评估的任务包括：

①识别构成风险的各种因素；

②评估风险发生的可能性和造成的影响，并最终评价风险水平或大小；

③确定组织承受风险的能力；

④确定风险消减和控制的策略、目标和优先顺序；

⑤推荐风险消减对策以供实施。

2.风险评估的内容：

①资产面临的威胁。Threats to its assets

②当前环境中存在的脆弱性。Vulnerabilities present in the environment

③威胁真实发生的概率（定量评估的频次）。The likelihood that a threat will be realized by taking advantage of an exposure (probability and frequency when dealing with quantitative assessment)

④威胁发生带来的影响。The impact that the exposure being realized will have on the organization

⑤消减措施。Countermeasures available that can reduce the threat’s ability to exploit the exposure or that can lessen the impact to the organization when a threat is able to exploit a vulnerability

⑥剩余风险。The residual risk (e.g., the amount of risk that is left over when appropriate controls are properly applied to lessen or remove the vulnerability)

3.定量风险分析/必考

要计算出具体的概率百分比，用货币形式表示每个资产和威胁。虽然，纯粹的、精准的定量分析是不可能的，但还是能用的。下面是定量风险分析的六个主要步骤或阶段，都不难理解：

①列出资产清单并分配资产价值，即 AV（asset value）；

②研究生成每个资产所有可能威胁的列表。为每个威胁计算暴露因子 EF（exposure factor）和单一损失期望 SLE（single loss expectancy），就是单损。

EF 也称为潜在损失，是该风险实际发生时，可能损失的资产价值的百分比。

SLE 就是该风险实际发生 1 次时，可能损失的资产价值，也就是损失多少钱。

SLE=AV×EF

③计算每种风险的年发生概率 ARO（annualized rate of occurrence）。

ARO 就是该风险每年可能发生几次，值从 0 到无穷大，越大越危险。如果风险每年发生很多次，它带来的损失可以远远超出相关资产的价值。

④计算每个风险的年度损失期望 ALE（annualized loss expectancy），就得到每个威胁可能的总损失。

ALE=SLE×ARO

⑤研究每个威胁的对策，然后基于对策，计算采取措施后的 ARO 和 ALE。

不管有没有采取措施，EF 是不变的，也就是不管攻击搞没搞成，反正只要搞成了，你就会损失这么多。安防措施的目的应是减少 ARO，就不让风险实际发生。

⑥针对每个资产的每个威胁的每个对策执行成本/效益分析。选择对最适用的对策。

这里要先计算每个威胁采取某种防护措施的年度成本 ACS（annual cost of safeguard），

部署安防系统的价值就是：施策前的 ALE—施策后的 ALE—ACS，可以让高层看到安防系统实现了多大的效益。SLE 和 ALE 的区别要搞清楚，经常考。

当然，除了算清楚钱，也要考虑法律因素、社会效益等，要采取“应尽关注”的态度，有些安防开支可以适度增加，不能只管赚钱。

4.定性的风险分析

不算钱，只是评估其风险、成本和影响，可以使用很多统筹学里用到的技术，如头脑风暴、得尔非（Delphi）、问卷调查、各种开会等。

①场景（Scenarios）

就是用一页纸讲清楚 1 个风险案例，用高、中、低或者 A、B、C 什么的表示影响程度。

②Delphi 技术

学过统筹学就知道，Delphi 技术就是一个简单的匿名反馈和响应过程。参与者通常被集中在一间会议室中，对每项意见或问题匿名反馈自己的想法；然后组织者修改完善这个报告或方案，再进行匿名反馈；最后所有参与者都答成一致，没有意见了。

③风险评估矩阵

横轴是风险影响，一般分 5 级；纵轴是风险发生的可能性，一般分 5 级。然后就得到了每个风险的评级。

5.其它

风险评估的方法论（模型）有：

①**FRAP**(Facilitated Risk Analysis Process)：专用的定量方法，先进行预筛选以节省时间和金钱。

②**OCTAVE**(Operationally Critical Tbreat, Asset and Vulnerability Evaluation)：面向团队的方法，通过组织研讨会来评估组织风险和 IT 风险。

③**AS/NZS 4360**：澳大利亚和新西兰的一种业务风险管理评估方法。

④**FMEA**(Failure Modes and Effect Analysis)，失效模式和影响分析：利用组件的基本功能来识别缺陷及其影响的一种方法。

⑤**故障树分析**：分析具体缺陷在复杂系统中出现的根本原因的一种方法。

⑥**CRAMM** 中央计算和电信机构风险分析管理方法：Central Computing and Telecommunications Agency Risk Analysis and Management Method。

I.3 风险分配/接受 （例如：系统授权）

1.风险分析的结果有：

①所有资产的完整和详细的评估。

②所有威胁、风险、发生概率和一旦发生的损失的详细列表。

③针对特定威胁的防护措施和对策列表，并且标识出其有效性与 ALE（年损）。

④每种防护措施的成本/效益分析。

2.对风险的应对策略有四种：

①降低风险（Reduce or mitigate），就是风险**消减**，采取最佳性价比的安防措施。

②转移风险（Assign or transfer），就是买**保险**或外包，自己不干有风险的事。

③接受风险（Accept），组织机构**书面**说明对某风险不采取任何措施，比如容忍地震。

④拒绝风险（Reject or ignore），最消极的态度，就当风险不存在，无视，**不管**它。

3.剩余风险

实施并实现了安防措施，仍然继续存在的风险被称为剩余风险，也是高层管理部门选择接受的风险。这也表明通过成本/效益分析，发现某些防护措施并不划算。

首先算个总风险：就是在没有任务防护措施的情况下，组织将要面对的风险数量，与威胁、脆弱性和资产价值有关。

然后算个控制间隙(controls gap)：就是通过采取防护措施被减少的风险数量。总风险和剩余风险之间的差值被称为控制间隙。代表了安防系统的效益，也就是可控制风险。

总风险-控制间隙(可控风险)=剩余风险。

I.4 风险应对策略选择

选择风险应对措施的原则主要有以下几个：

①措施的成本要小于资产价值。为办公室修个地下防空洞肯定是没必要的。

②措施的成本要小于措施的效益。雇用 1 个中南海保镖做公司门卫也是没必要的。

③措施的结果应当使攻击成本大于攻击获得的效益。压缩包加密就行了，要十年才能破解。

其它的原则就不列举了，自己看着办。

I.5 实施

就三类应对措施：

1.技术

包括：用户名、密码、智能卡和生物识别、加密、受限接口、访问控制列表、协议、防火墙、路由器、入侵检测系统（IDS）以及阈值级别。

2.管理

主要关注人员与业务，包括：策略、过程、雇用准则、背景调查、数据分类和标签、安全意识和培训效果、休假记录、报告和回顾、工作监督、人员控制以及测试。

3.物理

防止最直接访问和接触，包括：保安、围墙、移动探测器、闭锁的门、密封窗、灯光、线缆保护、笔记本电脑锁、磁条卡、看门狗、摄像机、陷阱以及报警器。

I.6 控制措施的类型 （预防措施、 检测措施、 纠正措施等）

1.访问控制的 7 个主要类型/安全控制功能种类：

①管理（Directive）/指引：指令性、强制性的规定，如：安全策略需求或标准、张贴通告、疏散路线出口标志、监控、监督、工作任务过程。

②威慑（Deterrent）：旨在打击潜在的攻击者。吓唬人别搞坏事，如：策略、安全意识培训、锁、围墙、安全标识、保安、陷阱、安全摄像机。

③预防（Preventive）：旨在避免发生事件。阻止非法进入，如：围墙、锁、生物测定学、陷阱、灯光、警报系统、责任分离、工作轮换、数据分类、渗透测试、访问控制方法、加密、审计、使用安全摄像机或闭路电视(CCTV) 、智能卡、回叫、安全策略、安全意识培训、反病毒软件、防火墙和入侵防御系统。

④补偿（Compensating）：提供可替代控制措施。增加访问控制措施，如：对 PII（个人信息）加密。

⑤检测（Detective）/监测：确认事件的活动和潜在的入侵者。发现非法进入，如：保安、移动探测器、记录和检查安全摄像机或闭路电视捕获的事件(CCTV) 、工作轮换、强制休假、审计跟踪、蜜罐或蜜网、IDS、违规报告、对用户的监管和检查、事故调查。

⑥纠正（Corrective）/矫正：事件发生后，修复部件或系统。发生非法访问后，将系统还原至正常的状态，如：终止恶意行为或重启系统、删除或隔离病毒。

⑦恢复（Recovery）：目的是使环境恢复正常运作。比纠正性控制更高级、更复杂，如：备份和还原、容错驱动系统、系统镜像、服务器群集、反病毒软件以及虚拟机影像。

很多安全措施是同时符合以上多种类型的，如果问 CCTV 是预防、还是威慑、还是检测？就要看题目中的场景了，它发挥的实际作用是什么就选最佳答案。

I.7 控制措施评估

看看第六域就行了。

I.8 风险监控与测量

安全控制措施必须是可以监测和度量的，否则并提供任何安全性。也就是安防系统的功能有效性和好处要能被看到。

I.9 资产评估

没什么要考的内容。

I.10 汇报

一个风险报告应该是准确、及时、全面的，能为整个组织提供清晰和准确的决策支持，并且定期的更新。例如，美国政府机构被要求在发现个人信息泄露的 1 小时内，向美国计算机应急小组(US-CERT)汇报。

I.11 持续改进

持续改进广泛使用的工具是四步质量模型，PDCA（计划——执行—评估—行动），也称为戴明环或休哈特环，这个在各种领域用的太多了：

①计划：识别时机并计划改变

②执行：小范围内实施改变

③检查：用数据分析改变的结果，确定是否有差别

④行动：如果改变是成功的，在更大范围内实施它和持续评估结果；如果这个改变无效，再次开始循环。

其他广泛使用的持续改进方法有：六西格玛，Lean 等。

I.12 风险框架

风险框架是关于如何评估风险、解决风险和监管风险的指导或方法。CISSP 考试主要考美国国家标准技术研究所(NIST) 在 800-37 专业出版中的定义。其它的企业风险管理（ERM）框架有：

1. COSO：2013

2. ISO 27005：2008
3. AS/NZS and 31000：2009
4. ISO Guide 73：2009
5. NIST Special Publications 800-37 and 800-39
6. ISACA (2009) Risk IT Framework

详细看第 9 域。

J. 理解与运用威胁建模

威胁建模是指潜在威胁被识别、分类和分析的安全流程。它通过寻找系统潜在的威胁以建立对抗的策略和安全的系统，使您可以对最可能影响系统的威胁进行识别和评价。

①威胁建模的**主动式方法**发生于系统开发的早期阶段，也被称为防御方法。事先集成安全解决方案更符合成本效益，比后面硬塞的方案更成功。但是，并不是所有的威胁都可以在设计阶段预测出来，所以仍然需要被动式威胁建模来解决不可预见的问题。

②威胁建模的**被动式方法**发生在产品被创建和部署之后，也被称为对抗的方法。通常需要在部署后精心制作产品的更新或补丁，有可能会牺牲一些功能性和用户友好性。

J.1 识别威胁 （例如：竞争对手、承包商、员工和可信合作伙伴）

1. 识别威胁的结构化方法主要有：

①关注资产

对资产进行估值，并试图识别对于宝贵资产的威胁。

②关注攻击

假设有潜在的攻击者，并基于攻击者的目标识别他们所代表的威胁。

③关注软件

主要考虑企业内部各种软件系统的潜在威胁。

2. 对威胁进行分类

通过常使用微软的 STRIDE 威胁分类方案（6 个首字母）。即：

①电子欺骗（Spoofing）——通过使用伪造身份获得对目标系统访问权限的攻击行为。可使用 IP 地址、MAC 地址、用户名、系统名称、无线网络名称、电子邮件地址以及许多其它类型的逻辑标识来欺骗。

②篡改（ Tampering ）——任何对数据进行未授权的更改或操纵的行为，包括在传输中的和被存储的数据。这种攻击主要侵害完整性和可用性。

③否认（ Repudiation ）——用户或攻击者否认执行了一个动作或行为的能力。也就是抵赖、不承认有过非法行为。

④信息披露（ Information disclosure ）——将私人、机密或受控信息揭露、传播给外部或未授权实体的行为。

⑤拒绝服务(DOS) ——指攻击试图阻止对资源的授权使用。这可以通过缺陷开发、连接重载或流量泛滥实现。DOS 攻击并不一定会导致对一个资源的完全中断；而是会减少吞吐量或造成延迟，以阻碍对资源的有效利用。

⑥权限提升(Elevation of privilege) ——此攻击是指有限的用户帐号被转换成一个拥有更大特权、权力和访问权的帐户。

一骗二改三抵赖；窃密瘫痪提权限。

3.威胁的优化级排序

对威胁进行排序或定级，可以利用 3 种技术来完成：

①概率×潜在

使用一个代表风险严重程序的编号，编号值从 1 到 100，100 是最严重的；概率和损失的值从 1 到 10 。

②高/中/低

很简单，每个威胁都被标注为三种优先级标签中的一种。高优先级的需要立即解决。

③DREAD 评级系统

对每种威胁问五个问题，根据回答情况来评级：

1. 潜在破坏——如果威胁成真，可能造成的损失有多严重?
2. 再现性——攻击者重复利用这一漏洞有多复杂?
3. 可利用性——实施攻击有多难?
4. 受影响用户——多少用户可能受到攻击影响？(百分比)
5. 可发现性——攻击者发现该弱点有多难?

每个问题通过 H/M/L 或 3/2/1 的值来回答，从而建立一个详细的威胁优先级表。

J.2 确定和图解潜在攻击（例如：社会工程学攻击、电子欺骗攻击）

进行威胁建模，确定可能发生的潜在攻击，通常通过创建图表来完成，包括元素、数据流指向和特权边界等要素。

J.3 执行风险降低分析

执行风险降低分析，字面上写的是降低，其实是指对程序、系统或环境的细化、分解和分析，就是对风险的详细分析。目的是为了更好地理解产品内部逻辑和与外部的交互关系，并理解输入、处理、安全性、数据管理、存储和输出等详细过程。系统分解的越合理、越细致，就越容易识别威胁。在这个分解流程中，你必须了解五个关键概念：

信任边界——信任或安全等级发生改变的位置

数据流路径——数据在两个位置之间的流动

输入点——接收外部输入的位置

特权操作——比普通用户或流程有更大特权的任何活动，如修改系统参数等

安全立场和方法细节——安全策略、安全基础和安全假设的声明

J.4 风险补救技术和流程（例如：软件架构和运营）

没什么要考的内容。

K 整合安全风险考量至采购策略与实践中

采购流程

采购解决方案通常包括：征求建议书（Request for Proposal, RFP)，RFP 用来针对业务

问题或需求让供应商提供解决方案的，它为采购决策提供了框架，并能让解决方案的风险和收益在前期明确定义。RFP 要传达必要的安全需求，并要求得到有意义的和具体的答复，其中包括供应商将如何满足这些要求。

K.1 硬件、软件和服务

没什么要考的内容。

K.2 第三方评估和监控 （例如： 现场评估、文档交换与审查、过程/策略评审）

很容易。

K.3 最低安全要求

没什么要考的内容。

K.4 服务级别要求

1.服务水平要求(SLR)

服务水平要求的文档包含客户对服务的要求，并演变成安全水平协定草案。它定义了：

①详细的服务水平目标

②共有的责任

③其他的需求尤指一组客户

2.服务水平协定(SLA)

SLA 是一个 IT 服务提供者和客户之间的协定，可以包括多个服务或多个客户。它：

①描述 IT 服务

②描述服务水平目标

③明确说明 IT 服务提供者和客户的责任

3.服务水平报告

服务水平报告是对提供商交付约定的服务质量的能力进行调查并报告。

4.服务水平协议(SLA) VS 保证

SLA 定义供应商和客户间约定的性能级别和赔偿或处罚。然而，有 SLA 并不意味着供应商总能遵守 SLA。

保证只能通过检查、评审、和评估来获得。

L. 建立并管理信息安全教育、安全培训与安全意识

L.1 组织内所需的适当安全意识、培训与教育级别

1.意识 Awareness

安全培训的先决条件是意识。培养安全意识的目标是让员工高度重视安全的重要性，站在讲政治的角度把安全放在第一位，充分认识到他们的安全责任和义务，知道能做什么、不能做什么。许多工具都可以被用于培养安全意识，例如海报、通知、时事通讯文章、屏幕保护程序、T 恤衫、经理振奋人心的讲话、告示、演讲、鼠标垫、办公用品、备忘录以及传统的由教师引导的培训课程。

2.培训 Training

教训是教导员工履行工作职责、遵守安全策略并具备基本操作能力。要让新用户知道如何使用 IT 基础架构、数据存储的位置以及如何和为什么要对资源分类。意识和培训往往都是内

部提供的。

3.教育 Education

往往是由外部提供的，是一项更全面、更细致的工作，对学生或用户进行系统的教学，通常与用户参加认证考试、成为专家或寻求职务晋升关联。

搞清三者的区别，考题会要求选择某活动是属于其中那类？

L.2 定期评审内容相关性

意识、培训和教育必须进行周期性的、适时的评估，以保持与时俱进。

第二域　资产安全　（保护资产的安全）

Chapters 5 in OSG 7th

No Chapters in AIO 6th

该域的内容不多。但是很多 CBK 里有的、会考到的内容在你的教材和培训班里都没有讲！

A. 信息与支持资产的分类（例如：敏感性、关键性）

资产必须根据安全策略先进行分类并标记，资产一般包括：敏感数据、硬件和存储介质。

1. 敏感数据包括：

①个人身份信息

个人身份信息（PII）是任何可以识别或跟踪一个人的信息，包括姓名、社会保障号、出生日期、出生地、电话号码、电子邮件地址、邮寄地址、社会保障号、名字、信用卡账号、银行账号等；没有代表性的个人信息不是 PII，如：一个 MAC 地址、IP 地址、操作系统类型、最喜欢的度假地点、高中吉祥物的名字等等。

②个人健康信息

受保护的健康信息（PHI）是任何与某人健康有关的信息。

③专有数据

专有数据指的是任何帮助一个组织保持竞争优势的数据，如版权、专利和商业秘密等。

2. 数据分级

就是定义数据的保密等级，绝密、秘密、机密什么的，第一域 A 章节里讲过了。每个等级的数据都必须采取相应的保护措施。CISSP 考试中的所谓的“敏感信息”是指任何不能公开的信息。在第七域 E.5 章节也讲了分级与分类。

由于数据所有者最了解对数据的使用、以及数据对组织的价值，因而数据所有者应当决定数据的级别。保护数据机密性最好的方法是使用强大的加密协议。此外，强大的身份验证和授权控制能有效阻止未经授权的访问。

数据如何分级？要考虑以下 6 个方面的内容：

①谁将访问该数据。Who has access to the data?

②数据如何被安全处理。How the data is secured.

③数据将保存多久。How long the data is to be retained.

④采用何种方法废弃数据。What method(s) should be used to dispose of the data?

⑤数据是否应当被加密。Whether the data needs to be encrypted.

⑥数据的用途有哪些即如何使用。What use of the data is appropriate?

3. 谁来决定信息分级？

信息所有者决定信息级别；管理员来实施，确保分级以及相关控制；所有者定期检查确保信息正确的分级。

4. 设备的生命周期

①需求定义。Defining Requirements

②获取和实施。Acquiring and Implementing

③运作与维护。Operations and Maintenance

④废弃和销毁（退役）。Disposal and Decommission

B. 确定并维护所有权（例如：数据所有者、系统所有者、业务/任务所有者）

一、数据政策

数据政策是：一整套指导建立数据管理框架的高层次原则，能被用于解决诸如数据访问、相关法律、数据所有权和管理职责、数据获取等宏观战略问题。由于提供了高层次框架，所以数据政策应当是动态和灵活的，既聚焦战略性指导，又能够适应各类不同类型的项目以及潜在的新挑战。建立数据政策 establishing a data policy 要考虑的因素有：

①成本 Cost。②所有权和管理权 Ownership and Custodianship。

③隐私 Privacy。④责任 Liability。(以终端的许可协议形式实现)

⑥敏感性 Sensitivity。（要保护好涉密数据）

⑦现存法律政策的要求 Existing Law and Policy Requirements。

⑧策略和流程 Policy and Process。（合规的实施、政策修订和问题处置）

二、相关的角色

1. 数据所有者（data owner）

数据所有者是数据最终责任人，通常是首席执行官、总裁或部门主管。他负责定义数据类别、确定访问控制权限、确保给数据贴上合适标签。他们也要确保基于分类和组织的安全策略要求足够安全。数据所有者的 4 个责任目标是：

①确定信息对组织使命的影响。②了解信息的替代成本。

②决定在组织内外部哪些人需要该信息，以及在何种环境里信息应当被发布。

④知晓何时信息是不准确的，不再需要的，或应当被销毁。

这里强调一下 NIST-SP800-18 里的术语：

行为规则（rules of behavior）、接受使用策略（AUP-an acceptable usage policy）

它们的概念是一样的，安装软件和网上注册账号时都经常碰到，是指用户阅读了并同意系统的一系列要求（许可协议）。

2. 系统所有者（system owner）

系统所有者是拥有涉密系统的人。他的责任是：拟制、实施和维持系统安全计划。

系统所有者通常和数据所有者是同一个人。

3. 业务/任务所有者（Business/Mission Owners）

业务/任务所有者是指项目经理或信息系统所有者，它的责任和系统所有者有重叠。

业务所有者拥有的程序可能是由其他部门开发或管理的系统。技术人员过度严格的安全控制可能会影响业务人员的使用。

4. 数据处理者（Data Processors）

数据处理者是指处理数据的各类系统。不过，欧盟将数据处理者定义为人或实体。反正只要是查看或使用数据了，它就是数据处理者。

这里强调下经常考的 7 个安全港原则（避风港 Safe Harbor program）。这是美国贸易部的一个控制机制，防止未授权的信息泄露，相关的术语有：

①通知 Notice：任何组织必须告知个人使用数据的目的。（告知我）

②选择 Choice：任何组织必须为个人提供可选择的机会。（我选择）

③向前传输 Onward transfer： 组织只有在遵守通知及选择规则的基础上才能向其他组织传输资料。（别乱传）

④安全 Security：组织必须保护好数据。（别泄密）

⑤数据完整 Data integrity：组织不得将信息用作其它目的，还要确保数据真实可信。（别乱改）

⑥访问 Access：个人可以查、改或删除任务组织所持有的他们的个人信息。（属于我）

⑦执行 Enforcement：组织必须落实以上各条原则。（别搞事）

数据出口方和进口方之间的合同必须事先获得国家数据保护当局的批准，方可传输出。

第一域 D.5 章节也讲到美国的安全港原则了。

有的考题会问道：The European Union (EU) Data Protection Directive’s seven principles。指的就是这 7 个东西。

5.数据管理员（Administrators）

负责分配数据权限，通常使用基于角色的访问控制模型来分配权限。

数据管理员的责任目标：

①明确地定义与功能相关的角色。②在项目的所有阶段建立数据的所有权。

③注重数据可审计性。④在可持续的基础上确保良好的数据质量和对元数据的度量。

6.数据保管者（Custodians）/监管员

数据所有者将日常任务委任给保管者，保管者通过合理的数据保存和保护，协助保护数据的安全和完整。技术人员或安管通常会成为保管人，很可能与上面说的管理员是同一人。

数据监管员的责任目标：

①遵守正确的、相关的数据政策和数据所有权指南。

②确保合法用户对数据的访问，维护数据集的安全。

③数据集的基础维护工作，包括但不限于数据存储和归档。

④更新维护数据集文挡。⑤保障数据集的质量，验证相关更新，并定期审计其完整性。

7.用户（Users）

用户就是使用系统、获取数据并完成工作任务的人。和上面的业务/任务所有者有点区别。

三、质量控制/质量保障 QC/QA

质量控制/质量保障机制是为了防止数据被污染。

1.两类错误

数据污染可能发生在一个处理过程中或事件中，将以下两类基本错误导入数据集：

①记录错误 Errors of commission(授予错误)。数据在录入或转存时发生错误，可能由设备故障造成。这类错误很普通，也容易被识别，能够在数据获取过程中通过适当的质量保障机制 QA 来有效的减少错误，也可以通过数据获取之后应用数据控制流程 QC 来减少该类错误。

②遗漏错误 Errors of omission。常常包括对合法数据的不充分记录，这样会影响到对这些数值的解读。这样的错误可能很难被探测和矫正，但是通过严格的质量控制流程可以发现很多这样的错误。

数据的寿命与数据文挡化的水平成正比，确保良好的数据质量的关键在于**文档化**：没有好

的文档化，用户很难确定数据是否适合使用，监管者很难知道由谁执行了怎样的数据质量检查。

文档化有 2 种类型：

一是记录数据的所有变更。

二是通过元数据反映数据集水平。

2. 数据文档化的目标/好处

①保证数据的使用寿命，满足不同目的复用。

②确保数据用户理解数据内容、数据背景和数据集的限制。

③便于发现数据集。

④提高数据集和数据交换的互操作性。

数据需要按已经定义的规则和协议被精细管理，**数据标准**显得尤其重要。数据标准的好处包括：*更有效率的数据管理(包括更新和安全)；*促进数据共享；*提高数据质量；*提高数据一致性；*促进数据集成融合；*更好地理解数据；*改善信息资源的文档化。

C. 保护隐私

关于隐私详见第一域 H.6 章节，和第二域 A 章节。

C.1 数据所有者

详见 B 章节

C.2 数据处理者

详见 B 章节

C.3 数据残留

数据残留就是在数据被以某种方式擦除以后，仍然遗留的数据物理痕迹。掌握以下几个与销毁相关的术语：

擦除（Erasing）/删除

就是删除数据，很容易被恢复的。

清除/消除（Clearing）/重写

消除或重写，要多次反复重写数据，一般的工具是恢复不了数据的。但硬盘的“坏区”、SSD 等仍可能被恢复。（在同等密级的系统重用磁盘，只要做 Clearing 就行了）

根除（Purging）/彻底消除

比消除更强烈的一种形式。为了让存储设备能再次使用于非密环境，必须消磁、反复格式化填充等，很麻烦。（要在低等级的系统重用磁盘，必须做 Purging 才行。）

解除分类（Declassification）/给介质脱密

解除分类就是脱密，就是上面讲的这个清除（purging），是一样的，搞不清楚什么区别。脱密的成本比买个新盘还高，所以一般军方都是直接摧毁存储介质，不再做它用的。

净化（Sanitization）/给系统脱密

净化是指从系统或介质中拿走数据，确保不会以任何形式被恢复。有 2 种方式，一是上面讲的解除分类，不破坏介质；二是把系统的硬盘拿走或销毁，要破坏介质。

消磁（Degaussing）

针对硬盘进行消磁，同时也会破坏电路元件，但仍不能确保数据彻底没了。技术人员还可

以把盘片拆到另一个硬盘上来读数据。消磁对光盘什么的肯定是没用了。

破坏/销毁（Destruction）

销毁是介质生命周期的最后阶段，也是清除介质数据最安全的方法。包括 Overwriting 覆写、Degaussing 消磁、Encryption 加密、Media Destruction 介质销毁等。

考试中，处理数据残留问题的特殊方法有 3 种，当然最安全彻底的方法是销毁。如果云平台上的数据没用了，只能通过加密来保护，你根本不知道它存在哪。

C.4 数据收集限制

没内容。

D. 确保适当的数据保留（例如： 介质、 硬件、人员）

1.保留资产

包括记录保留、介质保留（也称硬件保留）、人员保留等形式。

记录保留指的是，保留和维护重要的日志信息，以供审计调查。

介质保留指的是，保管好涉密存储设备，直到它被合理净化。

人员保留指的是，员工必须签好保密协议（NDA），确保离职后不泄漏秘密。

不过保留时间太长了，成本很高，也会带来一些不必要的麻烦，法律上会没事找事。

E. 确定数据安全控制措施（例如： 静态数据、 传输中数据）

E.1 基准

基准/基线（base line）就是最低的安全标准，目标是建立最低安全控制措施。多层防御体系的第一道防线就是采用基础性的网络安全技术和方法，它们为构建的更先进、可靠的技术和方法提供了坚实的基础。基线目录列举并写明了各项安全控制措施的细节。

E.2 范围界定和裁剪

①范围界定 Scoping(选优)：企业根据实际条件、适用性等，选择运用最佳的安全标准。

②裁剪 Tailoring(改进)：企业根据需求和环境特点，对相关标准的具体措施进行优化。

上面两个动词一般用在宏观的管理层工作上，在考题中经常出现的另两个词是关于日志过滤、数据清洗等情景的，经常会遇到：

①过滤/设置阈值 Threshold

②裁剪/限定阈值 Clipping

后面这两个词的联系与异同在具体的练习题里去理解意会吧，我是做过习题才知道正解答案是什么，至于为什么也说不清楚。

E.3 标准选用

要熟悉很多标准以及负责这些标准的组织和实体。乱七八糟的，看第九域吧。CBK4 中文版第 158 页介绍了很多的标准，考试里的偏题、难题可能从中随便抽一个来考，懒得看了。

E.4 密码学（加密）

密码学在第三域 I 章节讲了很多，别的域也讲了，重点看第三域 I 章节。要搞清楚静态数

据加密和和数据传输加密算法之间（流加密）的差异。

加密数据的各种工具可分为 3 个大类：

①自我加密的 U 盘设备。

②介质加密软件。

③文件加密软件。

传输过程的加密可分为 2 大类（这个点在通信、加密、IPsec 里都会提到）：

①链路加密。加密所有数据。

②端到端加密。路由信息是明文的，仅数据是加密的。

F. 建立处理要求（例如：敏感信息的标示、标记、存储和销毁）

1. 敏感数据的管理流程

①标记（Marking）

可以用不同颜色的物理标签，更多的是用标题、注释、水印等数字标签。DLP 系统可以识别和利用数字标签来管理文档。

②处理

只有指定的人员才有敏感介质的访问权。应当对负责管理敏感介质的人员进行有关如何正确处理和标记敏感介质的政策和流程方面的培训。

③管理（Handling）

重点要管好数据的备份和导出。

④存储（Storing）

数据要加密，存储介质要安全。

⑤销毁（Destroying）

磁盘要消磁，固态盘要粉碎。

⑥记录保存/保留

信息和数据只应当在需要时被保存。组织可以根据行业标准或法规要求在一定期限保存/保留特定记录。

2. 其它

考试中还有这样的问题：

While incident management is concerned primarily with managing an adverse event,problem management is concerned with tracking that event back to a root cause and addressing the underlying problem.

问题管理比事件管理更深入，前者要分析问题根源和潜在隐患；事件管理仅处理安全事件。

第三域　安全工程（管理工程与管理）

Chapters 6,7,8,9,10,21 in OSG 7th

Chapters 4,5,7 in AIO 6th

A. 利用安全设计原则实施和管理工程过程

所有教程一上来就搞个 V 字模型，没什么意思。重点要搞清楚本章与安全管理、安全运营这 2 章的关系，以及本章内容与另外 5 章的交叉。这里是关于组织和实施信息系统的安全相关的工程项目的方法和原则。总的指导思想很简单：系统工程的每一个阶段和环节都要考虑安全。

1. 安全成熟度模型 SSE-CMM

描述了一个组织的系统安全工程过程必须包含的基本特征，和软件能力成熟度模型一样，也分了 5 级。0：初始级；1：可管理级；2：定义级；3：可预测级；4：最佳级。

具体怎么分级的，搞不清楚，反正不考。

2. 实现机密性、完整性和可用性可采取的措施

①限制（Confinement）

软件设计人员使用**进程限制**约束程序的操作。进程限制允许进程只能在确定的内存地址和资源中读取和写入数据，也就是常说的**沙箱**。操作系统或其他一些安全组件不允许非法的读/写请求。如果进程试图执行的动作超过了为其授予的权限，那么动作会被拒绝，并且系统将采取进一步的行动，例如记录违法行为的日志。

②界限（Bounds）/边界

为进程都分配 1 个授权级别，分级分域管理。在比较简单的系统中，可能只存在两个授权级别：用户和内核。界限为每个进程划分其使用的内存逻辑区域，不准许其他进程的访问。

③隔离（Isolation）

通过访问界限对进程进行限制的时候，进程在隔离的状态中运行。进程隔离能够确保任何行为只影响与隔离进程有关的内存和资源。隔离是一个稳定操作系统的重要组成部分之一。

三者的关系：通过访问界限对进程进行限制的时候，进程在隔离的状态中运行。

3. 访问控制

有两种控制：强制访问控制（MAC）和自主访问控制（DAC）。其中，DAC 的主体具有一些定义访问客体的能力。其实还有非自主的（UDAC）和基于角色的（RBAC）。

4. 信任与保证（Trust and Assurance）

保证 Assurance 是满足安全需求的置信度（可信度）；保证必须被持续地维持、更新和重验证。信任可以通过具体的安全功能集成到系统中，而保证是在现实世界对安全功能情况可靠性和可用性的评估。“保证”这个词在安全评估的各项模型和标准里会多次出现，它其实是指系统的安全性能到底靠不靠谱，有多大的概率能完成实施和实现？一般用几个等级来表示。

类似的关于评价的概念还有：

认证与认可（certification/accreditation）、

质量控制与质量保障（QC/QA）、

验证与确证（Verification/Validation）。

5. 隐蔽通道 Covert Channels

非通信的手段被用于传递信息，就是隐蔽通道。使用隐蔽通道提供了违反、绕过或回避安全策略而不被发现的一种方法。相应的，公开通道是一种已知的、预期的、被授权的、经过设计的、受监控的和受控的通信方法。隐蔽通道有 2 种类型：

①**计时**：时间隐蔽通道通过以一种可预测的方式改变系统组件的性能或更改资源的时间安排来传达信息。使用时间隐蔽通道通常是一种比较复杂的传送数据的方法，并且难以检测。

②**存储**：存储隐蔽通道通过将数据写入一个其他进程可以读到的公共存储区域来传递信息。当评估软件安全时，需要注重评估任意进程将信息写入到内存中任意位置时，是否可能被其它的进程读取。

隐蔽通信出现的原因有以下 3 种：

①产品开发过程中的疏忽。

②软件内实施的访问控制措施不应。

③两个实体之间存在共享的资源。

B. 理解安全模型的基础概念（例如：保密性、完整性、多层模型）

第一域“安全管理”讲了控制框架和威胁建模，都是宏观的，不局限于信息安全业务，是适用于整个 IT 业务或者生产业务的。第三域“安全工程”也要讲很多的框架和模型，但都是针对信息系统的，或者信息安全的。

安全模型是指导思想和实施依据。

在信息安全中，模型是对安全策略进行标准化、规范化描述的方法，可以是抽象的，也可以是具体的。它通过一组显式的规则让信息系统执行和落实安全策略的概念、过程和措施。后面讲的大部分所谓安全模型，基本上是针对访问控制来的。后面那么多模型的目的和意义其实并没什么，就是开发一个安全系统时，要参考借鉴这些理论来制定合理的安全目标、需求，采取合理的综合性的系统架构。“安全策略”描述安全要求是什么，而“安全模型”描述如何把要求转换成可执行和可审计的技术规范。

主体是请求访问资源的用户或进程；访问是对资源进行读或写操作；**客体**是被访问的资源。

信任传递：如果 A 信任 B，并且 B 信任 C，那么 A 信任 C。信任传递是一个严重的安全问题，例如中国的 A 是不能访问外国的 C 的，但是通过 B 翻墙就可以访问 C 了。

封闭系统：小范围、专有的、难集成、高安全。（闭源）

开放系统：大范围、通用的、易集成、易攻击。（开源）

一、安全模式（Security Modes）运行安全模式

美国政府批准和规定的四种可用于分类信息系统的安全模式：专-高-分-多

（1）专用模式 Dedicated Mode

相当于前面讲的单一状态系统。所有用户都级别一样，都有全部权限。

（2）系统调度的/系统高级模式 System High Mode

和专用模式差不多，唯一区别就是用户不是获取有所数据的权限，虽然用户级别一样，都有授权，但要根据“知其所需”原则，仅被授予部分信息的访问权限。

（3）分隔模式 Compartmented mode

和系统高级模式一样，用户仅被授予部分信息的访问权限。差别在于用户虽然级别一样，

但初始权限不再是一样的，访问权限在给用户授权时就限制死了。而上面那个模式的用户是拥有全部权限的，只在具体访问数据时，再判断有没有访问的必要和权力。它还有一个机制可以实现 1 个用户同时处理多个互相隔离的数据，称为分隔模式工作站（CMWs）compartmented mode workstations。

（4）多级模式 Multilevel Mode

这里用户就被分级了，有的用户就没有访问部分数据的级别。

这四个模式很绕，其实一点意义都没有，还要考。列个表吧：

模式/Mode	访问许可 permission	访问需求 need	能否访问 不同级别数据	概括
专用模式 Dedicated	全局权限	不区分	数据不分级	一锅端
系统**高级**模式 System High	全局权限	区分	不分级，按需访问数据	鸳鸯火锅按需吃
分隔模式 Compartmented	不同权限	区分	数据按权限分级	自助火锅分开吃
多级模式 Multilevel	不同权限	区分	数据分级	不同档次火锅店

除了以上的，还有两种：

（5）受控模式 Controlled Mode

在系统的硬件软件上，有更多有限数量的信任被置于多个等级。其结果是，对分类等级和级别有更多限制。

（6）受限的访问模式 Limited access mode

最小的用户级别并不清晰，最大的数据敏感度并没有根据敏感而分类。

二、要考的安全模型

先基础概念：

1.令牌、功能和标签 Tokens, Capabilities, and Labels

Token 安全令牌是一个与资源关联的独立客体，描述其安全属性。（单个，是客体的）

Capabilities 功能列表用于存储与多个客体有关的安全信息。（多个，是主体的）

label 安全标签是客体附加的永久部分。（不能修改，是客体的）

2.可信计算基 Trusted Computing Base

美国国防部的桔皮书将可信计算基(TCB)描述为硬件、软件和控制方法的组合，这个组合形成了一个实施安全策略的可信任基准。通常 TCB 组件负责控制对该系统的各种访问，确保系统的行为在所有的情况下工作正常并遵守安全策略。从某种意义上说，操作系统的内核就是 TCB。如果启用 TCB，那么系统就拥有一条可信路径、一个可信外壳以及系统完整性检查功能。

①可信路径(trusted path)是用户或程序与内核之间的通信通道。TCB 提供保护资源、以确保这个通道不会遭受任何方式的危害。

②可信外壳(trusted shell)意味着任何在这个外壳中工作的人都无法“逃出去”，其他进程也无法“闯进来”。

③安全边界 Security Perimeter（与上一章中的界限 Bounds 概念不同）

TCB 与系统的其他部分的逻辑边界，TCB 通过严格可信路径（trusted paths）与外部通信。可信路径是建立在有着严格标准基础上的通道，它在不受 TCB 安全脆弱性影响的情况下准许进行必要的通信。

④引用监控器和内核 Reference Monitors and Kernels

TCB 进行访问控制最重要的组件就是引用监控器(Reference Monitor)，也称参考监视器，它是一个抽象机，是主体对客体进行所有访问的中介，不但要确保主体拥有必要的访问权限，而且还要保护客体不被未授权访问和破坏性更改。为了让系统能够获得更高的信任级别，就必须要求主体(程序、用户或进程)在访问客体(文件、程序或资源)之前取得完全授权。它处于每个主体和客体之间，并且在准许访问之前验证主体的访问凭证（令牌、列表、标签）。

⑤安全内核（security kernel）是使用引用监控器的 TCB 核心组件，是主体访问资源的中间人，通过可信路径与主体进行通信。安全内核由位于 TCB 内的硬件、软件和固件组件构成，并且实现和实施引用监控器概念。

3.安全模型

有的模型是概念模型，仅理论描述；有的模型是实际开发运用的，由开发者随便命名；有的模型是多功能的，是几种类型的混合。

①关于访问控制的：

*访问矩阵 Access Matrix models

*访问控制表 Access control matrix

*Bell-LaPadula 模型

*Take-Grant 模型

*状态机模型 State machine model，也是很多安全模型的基础

②关于完整性的：

*Biba 模型

*Clark-Wilson 模型

完整性模型有下列 3 个主要的目标：

- 防止未授权用户进行更改。
- 防止授权用户进行不正确的更改(职责分离)。
- 维护内部和外部的一致性(格式良好的事务处理)。

Clark-Wilson 实现了以上 3 个目标，Biba 只实现了第 1 个目标。

③关于信息流的：

*信息流模型 Information flow model，也是很多安全模型的基础

*非干扰/非相干模型 Noninterference model/Goguen-Meseguer 模型

*Brewer and Nash 模型（中国墙 Chinese Wall 模型）

*组合论 Composition Theories

④基于状态机的：

*Bell-LaPadula 模型

*Biba 模型

*Brewer and Nash 模型（中国墙 Chinese Wall 模型）

系统的状态是系统在某一时刻的即时快照。很多活动都会改变这个状态，这称为状态迁移(state transition)。实现状态机模型的开发人员必须标识所有的初始状态(默认变量值)，并且还要概括说明这些变量如何发生变化(可以接受的输入)，以使最终的各种状态(结果值)仍然

能够确保系统的安全。

⑤其它：

*Sutherland 模型

*Graham-Denning model 模型

*可信计算基 Trusted computing base，是建立大部分安全模型的基础

下面逐个介绍各种模型：

1.访问控制矩阵 Access Control Matrix

访问控制矩阵是一个由主体和客体组成的表，一一对应的表示每个主体对每个客体的操作权限。表的每一竖列都是一个访问控制列表（ACL），代表 1 个主体可以怎么操作的客体；表的每一横行都是功能列表/访问能力列表（capabilities list），代表 1 个客体可以被怎么操作。只有行或者列是不行的，因为要删除一个客体或主体的时候，必须用到行和列才能快速找出相关联的主体和客体，并作出相应的修改。在基于角色的访问控制系统中，这个矩阵的主体就是各种角色。

但它没有考虑主体（用户）间的关系，客体（数据）的共享，所以有了“取—予模型”。

2.取—予模型/Take-Grant 模型

Take -Grant 模型（获取-授予）采用有向图/定向关系图（导航图）来表示访问权限如何在主体中传递的。它有两个规则：具有授权资格的主体可以向另一个主体或客体授予相应的权限（授予 Grant）；具有获得权利的主体可以向另一个主体请求获得受益人权限（获取 Take）。此外，该模型还可以利用 1 个建立规则（create）和 1 个移除规则（remove）来生成权限和删除权限。自己可读可写，不管其它的人，是安定型（inert）；权限可以申请（取），也能分配（予），是变换型（transport）。①Grant；②Take；③create；④remove。

这种模型在各种系统的账户管理功能里经常用到，就是管理员可以分配下级用户，下级用户还可以分配子用户。

3.Bell-LaPadula 模型/BLP

也被称为多级安全系统（multilevel security system），两个专家搞的，美国国防部（DOD）用的的，为了解决机密性问题，防止信息从高流低。美军的信息分级是三级：非机密（公开）、机密、秘密以及绝密，前面讲过的。这个模型既是信息流模型，也是状态机模型，也是一种“主体-客体”模型，每个客体有个安全等级标签，每个主体要验证访问这个客体的权限后，才能实施相应的访问。它有三个著名的规则：

初级规则①简单安全规则（Simple Security Property）。不能上读（no read up）。

中级规则②*属性（星属性）规则（* Security Property）。不能下写（no write down）。也被称为约束属性(confinement property) 。

高级规则③强星属性规则（Discretionary Security Property）。主、客体必须同等级才能读写，通过访问控制矩阵/列表实现。也被称为自主安全属性规则（上级如果要给下级发文件，因为不能“下写”，所以要自主）。

Bell-LaPadula 只解决机密性问题，不支持完整性和可用性。它还不针对隐蔽通信，不适应用使用文件共享和服务器的现代系统。它应该和 Biba 模型对比来看。

4.Biba 模型

两个人为了商业应用，参考 Bell-LaPadula 搞的，主要目的是解决完整性问题，防止信息从低流高。这个模型既是信息流模型，也是状态机模型，也是一种“主体-客体”模型，每个客体有个安全等级标签。Biba 也有三大规则：

初级①简单完整性规则(simple integrity property)。不能下读（no readdown）。防止高级别数据被“污染”。

中级②*完整性规则(star integrity property)。不能上写（no write up）。

高级③引援/调用规则(invocation property)。主体不能请求（调用）完整性级别更高的主体的服务。

Biba 只解决完整性问题，也解决了调用的问题，不支持机密性和可用性。

它和 Bell-LaPadulap 这两个模型里的 property 翻译成属性、规则、原则、公理都行。“简单”就是读，“*星”就是写。

5.状态机模型 State machine model

无论处于何种状态，系统总是安全的。这种模型基于有限状态机(FSM)理论：

状态是系统在特定时刻的即时快照，包括各种指标参数；

安全状态是系统的某个状态的所有指标参数都是安全的；

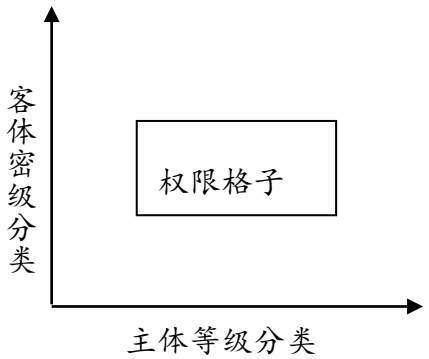
系统的任务操作和变化都用状态转换公式来表示：下一状态=F(输入，当前状态)；

所有的状态转换必须进行评估，如果系统的每一个状态都是安全的，系统被称为安全状态机（secure state machine）。

6.格子型访问控制 Lattice-Based Access Control

这里插播 1 个访问控制模型，本章讲的安全模型，绝大部分其实就是访问控制模型，这个格子模型也会被考到。格子型访问控制属于非自主访问控制（UDAC），不也就是说可以是强制（MAC）、也可以是角色（RBAC），反正就不是自主（DAC）。格子型也是信息流模型，主要解决机密性问题。

Bell-LaPadula 就是基于强制（MAC）和格子。这个格子就是指定 1 个主体所拥有权限的二维坐标（经纬度模型）；它不是一个坐标点，而是一个格子型的坐标面，这样主体能访问什么级别的数据很清楚了，高的低的都不能访问。（高不成低不就）



7. Clark-Wilson 模型

另一种用于商业的优秀模型，实现数据的完整性。其实就是 B/S 架构里的三层模型，有个中间件来实施访问控制。最重要的就是起“中间件”作用的 **TP**。先搞清几个术语和过程：

①用户 Users：活动个体 Active agents，也就是主体（数据项是客体）；

②转换过程(TP)Transformation Procedure：读、写、改操作，允许更改 CDI 的唯一过程；

③约束数据项(CDI) constrained data item：由 TP 控制，完整性被保护的任何数据项；

④非约束数据项(UDI) unconstrained data item：不受 TP 控制，用户直接操作的，完整性不被保护的任何数据项；

⑤完整性验证过程(IVP) verification and validation procedures：检查 CDI，确认其完整性的过程。

⑥受限接口模型（restricted interface model）：基于对主体、客体的分类，限制主体仅有用特定的访问授权。

Clark-Wilson 完整性模型的关键原理就是：通过 TP 限制对 CDI 的访问，即用户不能直接操作数据，必须通过身份验证后，根据授权通过 TP 来操作数据。该模型也要使用安全标签来授予对客体的访问权限，但只能通过 TP 过程和受限接口模型来完成。这种使用 TP 来操作 CDI 的机制也被称为格式良好的处理（well-formed transaction），它也实现了职责分离。

于是，这个模型中要实现一个成功的数据访问或修改，需要满足 3 个条件，所谓的访问三元组（access triple）：

①主体（Users）、②程序/过程（TP）、③客体（CDI）。

而且，优秀的完整性模型必须实现 3 个目标：

①防止未授权的更改；

②防止授权用户的不正当更改（职责分离）；

③保持内、外部数据的一致性（格式良好的事务处理）。

前面的 Biba 模型只实现了第一个目标。所以，银行肯定普遍运用了 Clark-Wilson 模型，它通过使用访问三元组(主体、软件(TP)、客体)、职责分离和审计来实现这 3 个目标。

8.信息流模型 Imformation Flow model

信息流模型以状态机模型为基础，后面的 Bell-LaPadula 和 Biba 模型都是信息梳模型。信息流的主要目的就是防止失泄密，也就是禁止出现未授权信息流，可以解决隐蔽通道的问题。当系统“状态”发生转换时，过程中一定有“信息流”的产生。

9.无干扰/无干涉/非相干模型 Noninterference Model/Goguen-Meseguer 模型

先讲讲推理攻击：指挥官在系统里可以看到部队要去俄罗斯打仗，小兵是看不到的，但小兵看到系统里关于俄罗斯普通信息突然增加了，于是就知道俄罗斯肯定有战事了。

无干扰模型参考借鉴了信息流模型，关注的是高级别主体的动作如何影响系统状态和低级别主体的，并不关注信息流。也就是说，高级别主体 A 的任何动作必须是无干扰的（不影响别人，也不受影响，避免出现泄密或隐蔽通信）；如果 A 能影响低级别主体 B 的状态（参考状态机模型），那么 B 处于不安全状态，可能归纳、推导出高级别信息。无干扰模型也可以防止木马危害。

Goguen-Meseguer 模型是一个完整性模型，没有 Biba 那么出名。它也被称为非干涉模型，因为它基于非干涉概念理论（noninterference）。GM 无干扰模型就要确保不同密级、不同归属的数据之间不能有任何的共享、关联和影响。具体怎么实现的，我也不知道。

10. Brewer Nash 模型（中国墙）BN

中国墙也是状态机模型，也是信息流模型。它根据用户的行为动态的进行访问控制，防止用户访问到会影响其它用户利益的敏感数据。所谓的墙，就是把有利益冲突的数据隔离开来，不允许同一用户访问，比如：公司的员工虽然有访问所有客户资料的权限，但根据业务记录，系统只允许他访问自己的客户 A 的资料，不能访问其它员工客户的资料，不然他就会抢别人的业绩了。

其它不考的模型：

11.组合论 Composition Theories

属于信息流模型，它关注多个系统间的输入/输出信息流（非单个系统）。因为它解释一个系统的输出如何关联影响另一个系统的输入，所以被称为组合论（集成、关联、组合）。

组合论有三种类型：

①级联(Cascading)：一个系统的输入来自另一个系统的输出。（单向流）

②反馈(Feedback)：两个系统来回流。（双向流）

③挂接(Hookup)：一个系统向另一个系统和外部实体都发送输入。（有出系统的流）

12.Sutherland 模型

Sutherland 模型是一个完整性模型，基于状态机模型和信息流模型，它用来防止隐蔽信道。该模型定义一组系统状态，只允许产生预定的安全的状态转换，具体的就不知道了。

13.Graham-Denning 模型（可能考）

Graham-Denning 模型主要用于删除或创建 1 个主体或客体，它定义了一组基本权限，即主体能够在客体上执行的一组命令该模型定义的 8 个关于增、删、改权限的基础原则。

14. Lipner 模型（Bell-LaPadula+Biba）

Lipner 以一种全新的方式把 Bell-LaPadula 和 Biba 模型的元素与职务功能或角色结合到一起，可同时保护保密性和完整性。发表于 1982 年的 Lipner 执行文件描述了实现完整性的两种方法。其中一种使用了 Bell-LaPadula 保密性模型，另种则同时使用了 Bell-LaPadula 模型和 Biba 完整性模型。这两种方法都给主体和客体分配了安全级别和功能类别。对于主体，这涉及一个人的许可级别和职务功能(如用户、操作员、应用编程员或系统编程员）。而对于客体，则根据其涉密级定义数据或程序及其功能的敏感性(如测试数据、产品数据、应用程序或系统程序)。Lipner 方法首先把客体划分成数据和程序。当从执行 Clark-Wilson 完整性模型的角度来看时，这个概念的重要性会体现得淋漓尽致：由于程序允许用户操控数据，对于用户可以访问的程序以及程序可以操控的客体实施控制，是非常必要的。

三、企业安全架构 ESA

考基本概念。

企业安全架构 ESA，是执行全机构信息安全基础设施的构件。ESA 侧重于为企业制定安全服务长期战略。它的主要目的是为安全服务开发确定优先重点，同时为信息安全方案计划提供输入信息。ESA 的重点是设计和执行通用安全服务以及实施受控安全区。这些方法的使用可帮助确保企业安全服务既有效，又能控制住成本。

ESA 的目标：

实现简单、长期的控制；It represents a simple, long term view of control,

提供统一、规范的控制；it provides a unified vision for common security controls,

基于现有的技术和成本；it leverages existing technology investments,

提供灵活的手段措施以应对当前和长远的威胁，并满足核心功能需求。it provides a flexible approach to current and future threats and also the needs of core functions。

具体相关的企业安全框架、标准和最佳实践在第一域讲了，这里再强调，详细见第 9 域：

1.企业架构 Zachman

表述企业架构基本元素的世界标准。

2.不同角度的企业安全架构

①中小企业，要保障业务需求的：

舍伍德应用业务安全架构 SABSA，Sherwood 应用业务安全架构。它是六个层级的框架。

②从不同部门、角色的角度考虑的：

开放组织架构框架 TOGAF。

③以软件系统为主要业务的：

软件定性分析系统架构描规范 ISO/IEC/IEEE 42010：2011。

四、安全相关的框架

有 COSO、COBIT、ISO27000、17799、ITIL、ISF 什么的。

C.基于系统安全评估模型选择控制措施和对策

这里讲如何选择安全模型和制定安全措施，也就是系统评估方法，其实是安全系统的各种评估标准。很多国内教程都有一个演变图：

欧洲的 ITSEC（90）

美国的 TCSEC 桔皮（85 年）=>美国的 FC（91）===>通用准则 CC（95）=>ISO-15408（99）

加拿大的 CTCPEC（90）

1.彩虹系列 TCSEC

美国国防部(DOD)和美国国家计算机安全中心(NCSC)在 80 年代搞的可信计算机系统评估标准(TCSEC) Trusted Computer System Evaluation Criteria，用不颜色的封面来发布不同版本的文件。最重要的就是橘皮书。

90 年代，英国等其它欧洲政府和机构在彩虹基础上搞出了信息技术安全评估标准(ITSEC) Information Technology Security Evaluation Criteria。

最后，这 2 个都被通信准则（Common Criteria）取代了。

其实具体行业也有相应的评估标准，如银行业的 PCI－DSS，很多地方会用到。

2.TCSEC 可信计算机系统评估标准 Trusted Computer System Evaluation Criteria

称为橘皮书，在产品评估中引入了可信计算基（TCB）的理念，用于没有联网的单机独立系统，从 4 个方面评估（安全政策、可控性、保证能力、文档）定义了 4 级 7 类的安全级别：

最低保护	D	最低保护，Minimal Protection；不满足安全要求
自主保护	C1	自主安全保护，Discretionary Security Protection；区分用户或用户组自行管理
	C2	受控访问保护，Controlled Access Protection；管理用户的权限、必须消除介质
强制保护基于 Bell-LaPadula	B1	**标签式**安全，Labeled Security；主、客体安全标签相符才能访问
	B2	**结构化**保护，Structured Protection；除了安全标签还要职责分离
	B3	**安全域**，Security Domains；职责分离更彻底(有安全管理员)+可信恢复
已验证保护	A1	验证设计 Verified Design；同 B3,系统开发-使用每个阶段都被评估验证

彩虹系统都过时了，但还是会考到：

红皮书/可信网络解释 TNI（Trusted Network Interpretation of the TCSEC），用于联网的系统，有四个级别：None、C1(Minimum) 、C2(Fair) 以及 B2(Good) 。

绿皮书（Department of Defense Password Management Guidelines）国防部密码管理指导原则，提供了创建和管理密码的指导原则。

TCSEC 之所以被取代了，因为它有以下不足：

①只管访问控制，不管获权后的用户行为；用户如何处理信息？这个问题没有考虑。

②只管保密，不管数据的准确性、完整性；因为 TCSEC 来源于军方。

③只管技术，没涉及管理、人员、实施、物理等方面。

④只管单机，没讲网络。

3.ITSEC 信息技术安全评估标准 Information Technology Security Evaluation Criteria

橘皮书只解决了机密性，ITSEC 则增加了对完整性和可用性的保证。

ITSEC 是欧洲最早的安全评估标准，对系统的安全机制区分**功能性**和**保证性**分别进行评估，被评估的系统称为评估目标(TOE)target of evaluation，TOE 的等级如下：

F1-F10 代表安全功能怎么样；E0-E6 代表安全功能被认可的级别（被信任程度）。

ITSEC 与 TCSEC 的差异：

①ITSEC 不止关注机密性，也关注完整性和可用性。

②ITSEC 不依赖于 TCB 的概念，不要求系统安全组件在 TCB 里被隔离。

③ITSEC 要求发生任何变化，系统都要重新评估；TCSEC 则不用。

表 4-3 ITSEC 和 TCSEC 的映射关系

ITSEC	TCSEC
E0	=D
F1+E1	=C1
F2+E2	=C2
F3+E3	=B1
F4+E4	=B2
F5+E5	=B3
F5+E6	=A1
F6	=提供高完整性的系统
F7	=提供高可用性的系统
F8	=在通信期间提供数据完整性的系统
F9	=提供高机密性(如密码设备)的系统
F10	=对机密性和完整性有高要求的网络

其中，F（功能性）里 F1 到 F10 对应的功能都在表里(F1-F5 就是 TCSEC 里的 D 到 A)。

那么 E（评估准则），也就是能力水平级别方面，E1 到 E6 是这样的：

E1：测试；E2：配置控制和可控的分配；

E3：能访问详细设计和源码；E4：详细的脆弱性分析；

E5：设计与源码对应；E6：设计与源码在形式上一致。

除了欧美，加拿大也搞了标准：CTCPEC，与 ITSEC 类似，将安全分为功能性需求和保证性需求两部分。其中，功能性要求分为 4 个大类：①机密性；②完整性；③可用性；④可控性。级别分为六级：0-5 级。

4.通用准则 Common Criteria

通用准则（CC）是全球性的系统评估标准，定义了测试和确认系统安全能力的各种级别，被设计用做产品评估模型，对功能性和保证性都进行评估。CC 全面考虑了与信息技术安全性有关的所有因素，符合 PDR 模型（防护、检听、反应）和现代动态安全概念。ISO 将这个准则文档命名为 ISO 15408“信息技术安全的评估标准”的官方标准。通用准则的 2 个关键元素：

保护轮廓(**PP**s) Protection profiles：被评估产品(TOE)的安全需求。（书上翻译的不好，这个 profiles 其实是指“安全需求规格说明书或概要说明”，AIO 里翻成保护样板了，官方习题集翻译成保护配置模板）

安全目标(**ST**s) Security targets：安全产品的供应商能提供的安全防护能力水平。

总之，你提供的安全产品（STs）要能满足我的安全需求（PPs），也就是要选择符合通用准则里相应等级的供应商。家里搞装修买复合板时，可以买欧标 E0 级别的，也可以买 E1 级别的，只不过 E0 含甲醛更少。

CC 包括 3 部分主要内容，即 ISO/IEC15408 的 3 部分：

①15408-1：**入门**介绍和通用评估模型，一般性的概念、原则、背景。

③15408-2：安全功能组件，定义要评估的安全**功能要求**。

③15408-3：安全保证组件，定义要评估的安全**保证要求**。

CC 的 7 个评估保证级别（EALs）evaluation assurance levels

CC 含有规格说明“包”，产品要想获得相应的等级，必须满足相应“包”中的规格说明。这些等级和这些“包”统称为 EAL。

EAL1：功能测试，Functionally tested

EAL2：结构测试，Structurally tested

EAL3：系统地测试和检查，Methodically tested and checked

EAL4：系统地设计、测试和检查，Methodically designed, tested,and reviewed

EAL5：半正式的设计和测试，Semi-formally designed and tested

EAL5：半正式的验证设计和测试，Semi-formally verified,designed, and tested

EAL7：正式的验证设计和测试，Formally verified, designed, and tested

功能➔结构➔系统测试➔系统设计➔半测➔半验➔正式验。（功能结构统统办办证）

表 8.4—安全评估标准的比较

TCSEC	ITSEC	CC	指定名称
D	F-D+E0	EAL0，EAL1	最小化/无保护
C1	F-C1+E1	EAL2	自主安全机制
C2	F-C2+E2	EAL3	受控访问保护
B1	F-B1+E3	EAL4	标签化安全保护
B2	F-B2+E4	EAL5	结构化安全保护
B3	F-B3+E5	EAL6	安全域
A1	F-B3+E6	EAL7	已验证安全设计

通用准则 CC 已经是最优秀的评估标准了，但也有缺点的：

①并不确认用户对数据的处理方式也是安全的。

②不解决技术以外的管理问题，也不涉及人员、机构和物理方面的安全问题。

③对加密算法的强度没有明确的等级评定。

5.认证和认可 Certification and Accreditation/认证与鉴定/信息与保证

对安防系统的正式评估过程包括两个阶段：认证和认可。

①认证：就是通过了技术评估，得到了安全等级证书。

②认可：就是通过了管理层的调查和审批，确定可以被实施。

认证 Certification　验证 Verification　确证 Validation　认可 Accreditation　维护 Maintenance，

这几个概念经常用到。第一域也提到了信任与保证(Trust and Assurance)。保证 Assurance 是满足安全需求的置信度（可信度）；保证必须被持续地维持、更新和重验证。信任可以通过具体的安全功能集成到系统中，而保证是在现实世界对安全功能情况可靠性和可用性的评估。“保证”这个词在安全评估的各项模型和标准里会多次出现，它其实是指系统的安全性能到底靠不靠谱，有多大的概率能完成实施和实现？一般用几个等级来表示。类似的关于评价与评估过程的概念在其它域多次出现，如：

*信任与保证（Trust/Assurance）；

*认证与认可（certification/accreditation）；

*质量控制与质量保障（QC/QA）；

*验证与确证（Verification/Validation）。

美国有 2 种标准用于信息系统的认证和认可：

①国防部使用国防部信息技术的安全认证和认可过程 DITSCAP（DOD information technology security certification），将认证认可划成 4 个阶段：

阶段 1：定义 Definition；

阶段 2：认证/验证 Verification；

阶段 3：确证/证实 Validation；

阶段 4：认可/发布 Post Accreditation。

②国家安全局使用国家信息保障认证和认可过程 NIACAP（national information assurance certification accreditation process），区分了 3 种类型的认可（鉴定）方式。

对系统的认可：a system accreditation，1 个单一的系统软件；

对站点/场所的认可：a site accreditation，1 个包含整套系统软件的站点；

对类型的认可：a type accreditation，1 个分布式的系统软件。

D. 理解信息系统的安全能力（例如：存储保护、虚拟化、可信平台模块、接口、容错）

其实就是了解各种安全系统所具备的主要功能特性，它实现了什么样的安全防护，有什么优缺点。

1. 内存保护

缓冲区溢出频发，安全架构师必须通过各种技术手段来保持主客体隔离以及各个主体之间的隔离，其中包括使用处理器状态、分层和数据隐藏等技术。

2. 虚拟化

虚拟机通常被隔离在一个沙箱环境中，若是受到感染，可迅速将其移除或关机，用另一台虚拟机取代。虚拟机对硬件资源拥有有限访问权，因此可帮助保护主机系统和其他虚拟机。

3. 可信平台模块（TPM）Trusted Platform Module（TPM=HSM）

TPM 是主板的加密处理器芯片，存储和处理密钥，以实现基于硬件加密系统。硬盘离开原来的系统，是不可能被解密的。TPM 是硬件安全模块(HSM)的一个典型应用。所谓的硬件安全模块 HSM，是一个用于管理/存储密钥、提高加密速度的硬件设备。许多认证系统使用 HSM 来存储证书；银行的 ATM 和 POS 终端通常采用专有的 HSM。

4. 接口 Interfaces

限制用户的权限一般通过限制应用程序的接口来实现，比如：一个普通用户没有权限，软件里相关的功能菜单就不会出现。Clark-Wilson 安全模型就运用了接口限制的技术。

5. 容错 Fault Tolerance

为了避免单点故障。具体内容在“灾难恢复计划”里。

E. 评估与缓解安全架构、设计和解决方案要素的脆弱性

先讲计算机硬件结构与运行原理。要了解软件是怎么在系统中运行的，才知道如何让它安全地工作。

一、硬件基础/计算机组成

1. CPU

中央处理器(CPU)，根据指令执行计算和逻辑操作。操作系统控制 CPU 的语言就是指令集。

CPU 的主要任务有 4 个：提取、解码、执行、存储。

CPU 的运行状态有 4 种（考点）：

*运行状态 Run or Operating state：执行指令。

*等待状态 Wait stage：等待特定事件完成。

*问题状态/运算状态 Application or Problem stage：执行应用程序（仅非特权指令）。

*特权状态/管理状态 Supervisor state：程序可以访问整个系统，可执行特权指令。

2. 存储器 Memory

①只读存储器

ROM（Read-Only Memory）ROM 有好几种：

PROM 可编程只读存储器 Programmable Read-Only Memory (PROM)，可烧入 1 次，不能改。

EPROM 可擦除可编程只读存储器 Erasable Programmable Read-Only Memory (EPROM)，可用紫外线多次改写。

EEPROM 电可擦除可编程只读存储器 Electronically Erasable Programmable Read-Only Memory (EEPROM)，可用直接多次改写。

闪存 Flash Memory，用的太多了，不解释。

②随机存取存储器 Random Access Memory

就是可读写存储器，掉电则数据无，也有很多种，不介绍了，有动态和静态 2 种：

动态 RAM：基于电容（capacitor），要不断刷新，成本低；

静态 RAM：基于触发器（flip-flop），速度快，成本高。

③寄存器 Registers

CPU 的核心，直接供算术逻辑单元 ALU 使用。

寻址/Memory Addressing 有 5 种方案，会考到的：

1)寄存器寻址 Register Addressing。寄存器是直接安装在 CPU 上的非常小的存储位置。当 CPU 需要从某个寄存器中获得信息来完成操作时，它可以使用寄存器地址(例如“寄存器 1”)去访问寄存器的内容。

2)立即寻址 Immediate Addressing（数据和指令在一起，不用寻）。就其本身而言，立即寻址并不是一个技术上的存储器寻址方案，而是引用某些数据的一种方法，这些数据作为指令的一部分提供给 CPU 使用。例如：CPU 可能处理命令“将寄存器 1 中的数值与 2 相加”。这条命令使用两个寻址方案。第一个方案是作为命令一部分的直接寻址，即告诉 CPU 将数值 2 加进去并且不需要从某个存储器位置中检索该数值。第二个方案是寄存器寻址，即命令 CPU 从寄存器 1 中取出数值。

3)直接寻址 Direct Addressing（地址和指令在一起，直接寻）。在直接寻址中，要被访问的存储器位置的实际地址会被提供给 CPU。这个地址必须与正在执行的指令位于相同的存储页面上。因为与重新编写立即寻址的硬编码数据相比，存储位置的内容能够被更容易地改变，所以直接寻址比立即寻址更灵活。

4)间接寻址 Indirect Addressing（通过指令里的指针去找地址，再通过地址找数据）。间接寻址使用的方案类似于直接寻址。但是，作为指令的一部分提供给 CPU 的存储器地址并不包含 CPU 用为操作数的真实数值。实际上，存储器地址中包含另一个存储器地址(也许位于不同的页面上)。CPU 通过读取间接地址来了解待操作数据驻留的位置，随后从这个地址中取出真实的操作数。

5)基址+偏移量寻址 Base+Offset Addressing（基址在寄存器中）。基址+偏移量寻址使用存储在某个 CPU 寄存器中的数值作为开始计算的基址。然后，CPU 将指令提供的偏移量与基址相加，并从计算得到的存储位置中取出操作数。

一个 CPU 有几种不同类型的寄存器，存储了需要执行的指令集和数据信息。

1)通用寄存器(general register)用于**保存变量**和临时结果。通用寄存器就像 ALU 在工作

时用到的记事本。

2)特殊寄存器(也称为专用寄存器)保存诸如**程序计数器、栈指针**和程序状态字(Program Status Word, **PSW**)之类的信息。

3)程序计数器，包含需要提取的下一个指令的存储器地址。执行这条指令后，程序计数器的内容就会更新为下一个需要处理的指令集的存储器地址。程序状态字(PSW)保存各种不同的条件位，其中一个条件位指出 CPU 应在用户模式(也称为问题状态)，还是在特权模式(也称为内核模式(kernel mode)或监管模式(supervisor mode))下工作。

④数据存储设备 Storage

主存 Primary：直接供 CPU 运算用的 RAM。

辅存/次存 Secondary：当前未被 CPU 使用的数据，外部存储，硬盘光驱什么的。

虚拟内存 Virtual memory：用辅存模拟额外的主存。

虚拟存储 Virtual storage：用主存模拟辅存，提高程序打开速度。

⑤输入/输出设备

键盘、打印机什么的，不讲了。重点讲输入/输出结构 Input/Output Structures：

存储映射 I/O，Memory-Mapped，在内存里使用一系列映射内存地址来访问外设。

直接内存访问(DMA) Direct Memory Access，不需要 CPU 处理，直接与内存交换数据。

关于存储的管理和控制这里不多讲，但很可能考到。

⑥固件 Firmware

固件是存储在 ROM 上的软件，很少被更改，前面讲的 EEPROM 就是固件。主要有两种：

计算机主板上的 BIOS 和和其它设备的固件（路由器、打印机、机顶盒）。

3.实现内存保护的三种最常用方法是：

①分区：分区是指把计算机内存划分成若干区段。指向一个内存位置的方法包括，用一个值标识一个区段以及该区段内的偏移。

②分页：分页是把内存地址空间划分成大小相等的叫做页的块。分页表把虚拟内存映射到物理内存上。分页表使附加内存的分配变得更容易，因为每个新页都可以从物理内存中的任何位置分配出来。一个页若是未被明确分配给一个程序，这个程序将不可能访问这个页，因为每个内存地址要么指向分配给该应用的一个页，要么生成一个叫做页错误的中断。未被分配的页和已经分配给任何其他应用的页不会拥有该应用接触得到的地址。

③保护键：保护键机制把物理内存划分成特意大小的块，每块都拥有一个叫做保护键的相关数值。每个流程还拥有一个与之相关的保护键值。当内存被访问时，硬件将检查，当前流程的保护键是否与将被访问的内存块的值相匹配如果不匹配，则会引起异常。

还有其它方法：

④地址空间布局随机化 ASLR

内存保护有其它附加技术手段，如地址空间布局随机化(ASLR)、可执行空间保护等。

ASLR 涉及在流程的内存地址空间随机安排程序的关键数据区的位置，其中包括可执行程序以及栈、堆和库的位置。地址空间布局随机化的依据是，攻击者猜出随机排列的区域位置的概率极低。增加搜索空间提高了安全性。

⑤可执行空间保护

把内存区域标明为不可执行，也就是说，在这些区域执行机器代码的任何尝试都会引起异常。许多 64 位操作系统通过某种形式的 ASLR 实施可执行空间保护，以此来预防某些种类的缓冲区溢出，如 return-to-libe 和 return-to-plt 攻击。

二、基本概念

①任务 tasking。执行一个程序就是一个任务。

②进程 processes。进程就是程序运行的动态过程，是独立运行的一个程序单元，存在内存里，是指令集和分配资源的集合，内存、CPU 时隙、API 接口、访问文件等都是资源；当进程有具体活动需要操作系统执行时，生成一个指令集给 CPU，这就是线程，活动完成线程即撤消。1 个程序可以作为多个进程在后台运行。进程有 3 个状态：就绪（等 CPU 时隙）、运行（执行）、等待/阻塞（等数据输入）。

③线程 threading。是进程中的一小段相对独立的代码，可重用也可并发运行，也是正在被 CPU 执行的一组指令集和数据。程序可以设计成多线程（Multithreading），这样同一个程序（进程）的不同功能模块（显示、打印、传输什么的）可以在多个不同的线程中同时运行。不过 CPU 最好具备多线程运算能力，不然那么多线程的效果发挥不出来。同一个进程的所有线程是共享存储资源的。

④多任务 Multitasking。同时执行多个程序，用于单机，由操作系统协同调度。有 3 种类型：实时多任务(Real time)、抢占式多任务(Preemptive)、协作式多任务((Cooperative)。没有“多进程”这个概念的，多进程就是多程序，对于单个 CPU 来说，也就是多任务，就是内存中加载很多进程。

⑤多线程 Multithreading。一般情况下，一个进程（processes）执行一个任务/程序（tasking），并生成一个线程(threading)等待 CPU 执行具体操作；而多线程就是指一个进程/程序被分成多个线程来执行。一个典型的例子：同时打开多个文档时，如果通过多个进程来实现，文档间的切换和交互需要更多的指令，速度慢；如果在同一个进程里生成多个线程来跑不同的文档，速度会快很多。

⑥多程序设计 Multiprogramming。用于大型机和分布式计算，自己编程来通过操作系统协同不同主机的运算，过时了。（使用 1 个 CPU 对多个程序进交叉存取执行）

多程序与多任务的区别：一是多程序通常在大型机中使用，而多任务在 PC 系统(例如 Windows 和 Li nux)中使用；二是多任务通常由操作系统协调使用，而多程序则要求特别编写的软件，这种软件通过操作系统来协调自己的活动和执行。

⑦多处理器 Multiprocessing。有 2 种方式使用和控制多个 CPU：一是对称多处理（SMP），单机用的，几个 CPU 共享同一个操作系统、内存和总线；二是大规模并行处理（MMP），大型机用的，每个 CPU 有自己的操作系统、内存和总线（要用多程序设计来控制）。补充：单个的四核 CPU 也算是多处理器，它相当于 4 个 CPU 的运算能力。现在常用的单机 CPU 具备 4 核 8 线程能力。

总之：任务是用户要系统做的操作；进程是后台内存里跑的程序；线程是 CPU 里运行的活动单元。【软件>程序/任务（内存）>线程>处理器（寄存）】

⑧中断(IRQ) Interrupt

中断是单个 CPU 实时地处理内部或外部事件的一种内部机制，就是申请 CPU 暂停正在执行

的程序，先把中断的事件处理完了，再回来断续。它为设备指派特定的信号线即中断号。

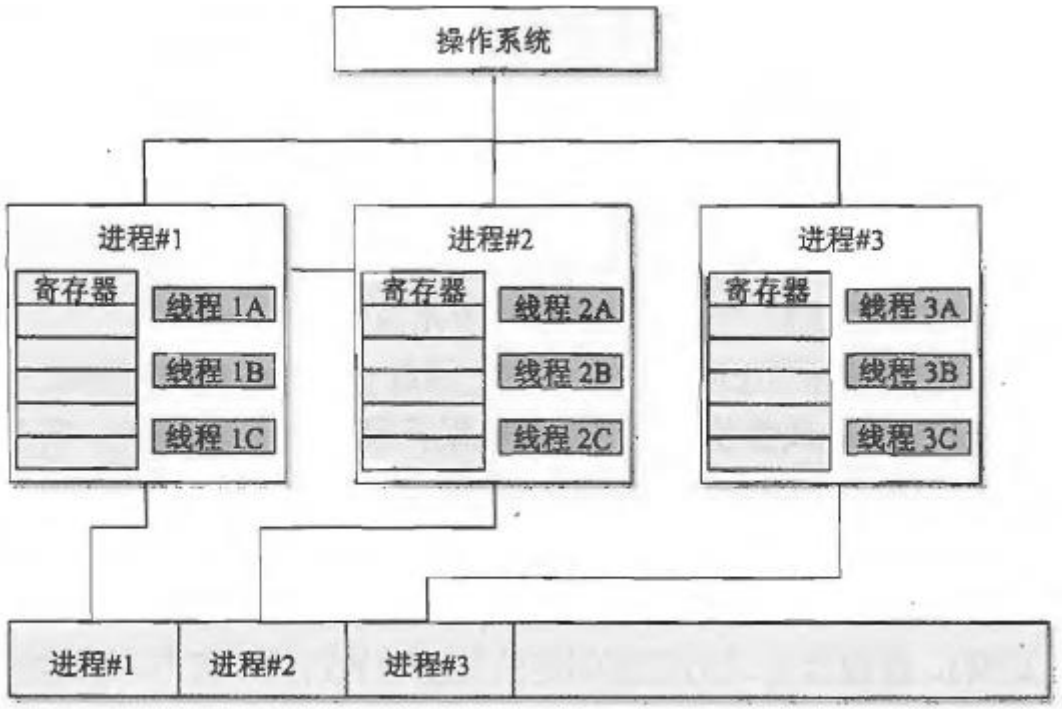


图 4-9　进程与线程的关系

三、操作系统/CPU 的运行机制

进程、线程什么的由操作系统控制，在 CPU 里运行，它本身是很大的安全风险的，因为存储的数据很容易被溢出、被篡改，进程、线程也可能被恶意控制、取代什么的。所以还要进一步深入学习操作系统。这里不能成体系的讲解，只能罗列相当的概念了。

1.操作系统的分层架构：

①单层操作系统（单块操作）：所有的操作系统进程在内核模式下运行。(MS-DOS)

②分层操作系统 THE(Technische Hogeschool Eindhoven 多程序设计系统)：所有的操作系统进程使用分层模式在内核模式下运行。THE 有 5 层：0 层访问 CPU；1 层管理存储器；2 层提供进程间的通信；3 层处理 I/O 设备；4 层驻留应用程序。

分层或环形的安全模型，只分了 4 层：

0 环：安全内核，1 环、2 环设备驱动，3 环执行应用，4 环以上不存在。

③微内核操作系统：关键操作系统进程在内核模式下运行，其余在用户模式运行。通过限制运行在内核模式下的进程的数量，使系统更为安全，减少复杂性，增加操作系统的可移植性。

④混合微内核操作系统(hybrid microkemel architecture)：所有操作系统进程在内核模式下运行，关键操作系统运行在微内核，其他使用客户端\服务器模式运行。操作系统服务是服务器，应用程序进程是客户端。

2.CPU 的 2 种操作模式：

问题状态/用户模式 User Mode：执行应用程序代码，支持部分指令，处理部分资源。

管理状态/特权模式 Privileged Mode/内核模式 kernel mode：执行操作系统代码，支持全部指令，处理全部资源。

这两模式在后面的环式模型里也讲到了。

3.信息系统的 2 处理方式：

①单一状态 Single State systems。系统一次只能处理同一个安全等级的信息。这确实简单、安全，反正高密的、低密的都进不来。不过效率低了点。

②多态 Multistate systems。不同安全等级的信息和操作同时在运行，不过都被互相隔离了。这个虽然系统运行效率高了，但安全方面的投入成本很很大，还不如多部署几套系统呢。

4.计算机的处理方式

有三种保护机制：保护环、进程状态、安全模式

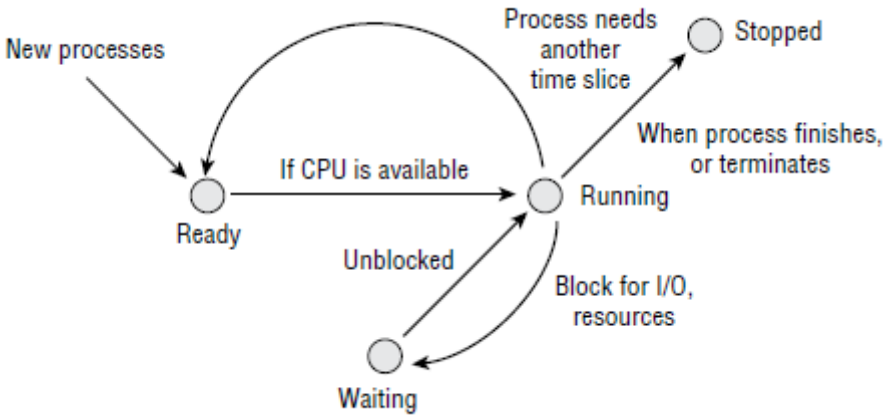
①保护环 Protection Rings。

最内部的环 0，有最高的特权级别.，可以访问任何资源，是操作系统的内核(kernel)。这个内核是指操作系统始终驻留在内存中的部分。环 1 是操作系统中没有常驻内存，用时才读入的部分。环 2 是 I/O 驱动程序和系统工具，可以访问外围设备和特殊文件。环 3 是一般应用程序什么的。环 0、1、2 被称为内核模式或特权模式，属于系统级的访问；环 3 以外被称为用户模式，属于应用级的访问。

外围环使用内部环的服务必须要提出申请，这部称为居间访问模型 mediated-access Model。（这个居间是对 mediated 的翻译，指位于中间的人，即起到协调作用的中介。）通过居间访问调用高级别的资源时，系统会检查并确认访问全体的身份和授权。

②进程状态

前面讲过进程有 3 种状态：就绪、运行和等待/阻塞。其中运行状态也被称为“问题状态”（problem state），是指计算机正在处理和解决某个问题，也指这个计算过程中是可能发生问题或错误的。



其实，进程还有 2 种状态：

监管 Supervisory：进程要使用比运行状态更高级别的资源（更改系统配置、安装驱动程序、更改安全设置什么的）时，就要使用监管状态。也就是环 3 模式（用户模式）或运行状态里不具备的功能，都要到监管状态下才有。

停止 Stopped：进程被终止，释放内存等资源。

E.1 基于客户端 （例如： 小程序、本地缓存）

这里讲针对单机的攻击和漏洞。

1.Applets

在本地单机安装的客户端软件（浏览器插件），为了更好的使用 WEB 服务，提供更多的功

能。有 2 种常用的：基于 JAVA 的 Java Applet 和基于微软.NET 的 ActiveX 控件。Java applet 和 ActiveX 控件的主要区别是 Java 为代码运行建立一个沙箱，并且限制代码访问用户计算机系统上的资源。ActiveX 使用依赖于数字签名和信任认证授权的身份验证码技术。尽管两者都是很好而有趣的技术，但是它们都存在内在的缺陷。Java 不能保证所有代码都在沙箱中运行，这容易引起几种类型的安全危害，这些危害都是恶意软件的示例。ActiveX 不一定提供安全性，事实上，它总是向用户弹出讨厌的警告对话框

2.本地缓存 Local Caches

①ARP 缓存中毒

ARP 协议是将 IP 地址解析为 MAC 地址的协议。这种攻击使客户端传输的数据流发送给不是预期的其它系统（另一个 MAC 地址），这种攻击也被用来做中间人攻击。动态 ARP 缓存：攻击者回应 ARP 广播查询并发送伪造的回复，这样 ARP 缓存一起缓存，直到超时（通常是 10 分钟）。静态 ARP 缓存：本地执行 ARP 命令，这需要通过木马、缓冲区溢出或社会工程攻击才能在客户端运行。

②DNS 缓存中毒

另一个比较流行的中间人攻击方式，类似于 ARP 缓存，让主机访问别的地址。主要手段有：主机中毒、授权 DNS 服务器攻击、缓存 DNS 服务器攻击、DNS 查找地址改变以及 DNS 查询欺骗。

主机文件 HOSTS file：将常用的或访问过的域名（域名也被称为 FQDN：fully qualified domain name）与 IP 地址的映射存储在本地，方便下次上网用，提高速度。修改这个文件就可以让访问重新定向。

授权 DNS 服务器攻击 Authorized DNS server：直接修改权威 DNS 服务器（根服务器）的数据库，于是全网的域名解析都被篡改了，很严重，所以很快会被发现并纠正的。

缓存 DNS 服务器攻击 caching DNS servers：运营商或企业为了速度，缓存了从其他 DNS 服务器获得的 DNS 信息，搞它要容易多了，也不易被发现。

DNS 查找地址改变 DNS lookup address changing：这个很直接，通过修改 DHCP 服务器或修改本地静态 IP 地址，篡改主机的 DNS 地址，让主机到另一个伪造的 DNS 服务器上去查询。

DNS 查询欺骗 DNS query spoofing：这个有点难，但也经常发生。攻击者截获主机的 DNS 查询请求，然后发回错误的结果，让主机访问错误的网站，把 DNS 服务器屏蔽了。

③Internet 临时文件中毒

上网浏览时，所有网站的内容都被缓存到本地的临时文件夹里。被植马的网站页面文件（图片、HTML 什么的）会被缓存到本地，然后就等待被调用或激活。

E.2 基于服务器端 （例如：数据流控制）

服务器的攻击和漏洞，大部分是针对传输的数据流的。这里没啥内容。

E.3 数据库安全 （例如： 数据推理、 数据聚合、数据挖掘、数据分析、 数据仓库）

数据库安全必考，基础内容看第八域 A 章节。

1.聚合 Aggregation

聚集攻击是通过收集大量的低安全级别的或低价值的数据，将它们结合起来，创造较高安全级别或有价值的信息。对于数据库来讲，就必须严格控制对聚合函数的访问并且充分估计可

能展示给未授权个体的潜在信息，这些对数据库安全管理员来说是特别重要的。

SQL 就供了许多可从一个或多个表中组合记录并生成有用信息的函数包括 count，mm，mate，sum，avg 等，这一过程就是聚合。数据库管理员应该严格控制聚合函数的访问，并且可以使用视图(view)的访问方式。防范聚合的对策有：

①基于内容的访问控制(Content-dependent access control)：根据数据本身的敏感度来管理访问控制。

②数据库分区技术可以防止聚合和推理。每个分区都具有唯一的、不同安全级别的内容。

③视图可以防止聚合攻击。在数据库中实现多级安全性的一种途径是使用数据库视图。视图可以整理来自多个表的数据、聚合单独的记录或限制用户访问数据库属性和/或记录的有限子集。在数据库中，视图被存储为 SQL 语句，而不是被存储为数据表。这样可以减少所需的数据库空间，并且允许视图违反应用于数据表的规格化规则。因为视图非常灵活，所以许多数据库管理员将视图作为一种安全工具使用，就是允许用户只与受限的视图交互，而非与作为视图基础的原始数据表交互。

④结合严格访问控制、“需知”和最小特权原则来预防聚合攻击。

2.推理 Inference

推理与聚合有点像，推理攻击利用几个非敏感信息片的组合，从而获得对应该属于更高级分类的信息。推理需要利用人的推断能力，而聚合只是简单的叠加。对于推理攻击的最好的防范是对有特权的个人用户保持持续的警惕。此外，数据的故意混淆可以被用来防止对敏感信息的推理。最后，你可以使用数据库分区帮助降低这些攻击。防范推理攻击的方法有：

①单元抑制(cell suppression)：隐藏特定存储单元的内容，限制用户对特定内容的访问。

②数据库分隔/分区(database partition)：把数据库逻辑分区，用视图来提供访问。

③噪声与扰动(noise and perturbation)：在数据库中插入伪造信息，误导和迷惑攻击者。

④基于上下文的访问控制(Contest-dependent access control)：根据访问的状态或者顺序来限制对某些内容的访问，需要一定的学习功能。

⑤基于内容的访问控制(Content-dependent access control)：根据数据本身的敏感度来管理访问控制。（信息分级）

⑥多实例（Plolyinstantiation）在同一个关系数据库表中两行或更多行（无组）具有相同的主键，且为不同密级的用户提供不同的数据查询结果，就是多实例。主要防范推理攻击。（这个点经常考到）

下面这些内容在第八域的数据库与数据仓库小节里详述。

3.数据挖掘 Data Mining

数据挖掘可用来揭示数据仓库中隐藏的关系、模式和趋势。很简单，不解释。讲下元数据的概念：就是描述数据的数据，或者关于数据的数据，也就是信息的数据。

4.数据仓库 Data Warehousing

将异构的，广泛分布的，很多的，独立的数据库关联到一起就成了数据仓库。

5.大数据、数据分析

联机事务什么的，没啥好说的。

E.4 大型并行数据系统

没啥考的。

E.5 分布式系统 （例如：云计算、 网格计算、 对等计算）

1.云计算 Cloud Computing

美国国家标准和技术研究所 NIST 把云计算定义为一种模型，包括五个基本特点、三个服务模型和四个配备模型组成。

五个基本特点：

①按需自助；②宽带网络访问；③资源池化；④快速弹性；⑤可计量的服务。

三个服务模型：

①软件即服务(SaaS)应用软件云：为用户提供直接可以使用的网络软件服务，一般基于浏览器。它的灵活性是比较低的，有什么用什么，综合性的比较少。

②平台即服务(PaaS)/平台开发云：为用户提供一个托管平台，承载用户自己的应用。在云基础设施上部署自己开发或采购的各种服务，必须遵守该平台的接口和环境如编程框架、数据存储模型等。

③基础设施即服务(IaaS)/基础设施云：为用户提供的是底层的、接近于直接操作底层服务接口，可以使用计算机资源、存储资源和网络资源等更多的基础资源。但软件全要用户自己来开发。

四个配备模型：

①专有云；②社区云；③公共云；④混合云。

2.网格计算 Grid Computing

网格计算是并行分布处理的一种形式。类似于通信里的自组网，联网单机只要空闲就可以加入网格群来完成个小任务。不过网络计算是全公开的，这并不安全，有的单机也可能出现问题而影响整个计算进度。

网格计算常常被与“集群计算”混为一谈，它们的区别是：

①这两种计算都涉及用两台或多台计算机来解决问题，但网格计算是异质的，而集群计算是同质的。

②网格计算机可以配备不同的操作系统、硬件和软件。

③网格计算机还具备多任务同时处理功能(一台计算机既是一个配有空闲CPU 资源的网格的组成部分，同时又可执行常规台式机功能)，而集群只用于一项任务。

④集群常通过连接节点的快速总线或网络把物理位置拉近，而网格则是在地理上散布的。

E.6 密码系统

看本域的第 I 章节。

E.7 工业控制系统 （例如：SCADA）

工业控制系统(ICS)

工业控制系统（ICS）Industrial Control Systems 是一种用于控制工业生产过程和机器的计算机管理设备。工业系统和关键基础设施通常由叫做工业控制系统(ICS)的简单计算机监测和管理。ICS 建立在标准嵌入式系统平台上，往往使用商业现货软件。ICS 是用于控制制造、产品处理、生产、配送等工业流程的。

ICS 类型包括：

①监测控制和数据采集/数据采集与监控系统(SCADA)系统。

②分布式控制系统/集散控制系统(DCS)。

③可编程逻辑控制器(PLC)。

④可编程逻辑器件(PLD)Programmable Logic Device，就是可编程的数字集成电路，可以完成大量的组合逻辑运算（与、或）。

其中 SCADA 用的最多，这个很厉害的，“震网”病毒就是通过它搞坏硬件基础设施，这里不多讲了。

F.评估和减缓基于 Web 系统的脆弱性（例如：XML,OWASP）

1.可扩展标记语言(XML)

XML 是万维网络联盟（W3C)的文本文件数据结构化标准，目的是使数据格式和数据可以在内联网和 Web 上共享。

标记语言，如超文本标记语言(HTML)，只是用于识别文档结构(格式)的一种符号和规则系统。XML 被称作可扩展，是因为符号是无限的，可由用户或作者定义。XML 格式可用独立于数据库、应用和所涉 DBMS 的一种中性格式来表现数据。

2.安全断言标记语言(SAML)

在第 5 域 B.6 章节重点讲了。

安全断言标记语言(SAML)是基于 XML 的一种用于交换认证和授权信息的标准。SAML 在设计上允许带不同身份管理系统的联邦式系统通过简化登录和一次登录交换进行交互。

尽管 SAML 的设计有着与生俱来的安全性，安全架构师还必须确保执行不会弱化该语言的安全。例如，当传递 SAML 断言，说明如果系统省略授权请求的标识符或接收者的身份，攻击者将能未经授权访问用户账号的时候。

3.OpenID Connect

OpenID Connect 是基于 OAuth 2.0 规范系列的一种可互操作的认证协议。它使用了直接 REST/JSON 消息流，设计目的是“让简单的事情简单，让复杂的事情变成可能。”

OpenID Connect 与 OpenID 2.0 在架构上有许多相似之处，事实上，这两个协议解决了非常近似的一组问题。然而，OpenID 2.0 使用的是 XML 和一种定制消息签名方案，而实践证明，开发人员有时很难把它搞定。因此，OpenID 2.0 的执行有时会神秘地拒绝互操作。OpenID Connect 则在需要签名的时候使用标准 JSON Web 令牌(JWT) 数据结构。这给执行 OpenID Connect 的开发人员带来极大便利，从而大大提高了互操作性。

如果要用户用 google 的账户来登陆一个网站，就用 OpenID。在第五域 B.1 章节计单点登陆里，提到了 OpenID。

4.开放 Web 应用安全项目(OWASP)/如何确保网站安全

在第八域 B.1 章节也讲了。OWASP 是一个致力于提高软件安全性的非营利机构。OWASP 开发了大量免费的实用产品，其中包括：

①OWASP 十大项目：基于 Web 应用存在的十大缺陷给出抑制它们的方法。

②OWASP 指南项目：一部说明如何设计出安全的 Web 应用和服务的全面手册。

③OWASP 软件保障成熟度模型(SAMM)：SAMM 是一个框架，用于针对机构面临的具体风险量体裁衣地设计软件。

④OWASP 移动项目：为开发人员和架构师开发和维护安全移动应用提供了资源。

有鉴于基于 Web 和基于云的解决方案使用得非常普遍，OWASP 提供了一个带 Web 应用安全流程的可访问全面框架。你应该对 OWASP 的作品有一个全面的了解，搞清如何将其应用到自己的任务中。OWASP 识别出的 10 大顶级风险有：

A1：注入；A2：跨站脚本攻击(XSS)；A3：无效的认证和会话管理；

A4：不安全的直接对象引用；A5：跨站请求伪造(CSRF)；

A6：安全配置错误；A7：不安全的加密存储；A8：URL 访问限制失败；

A9：薄弱的传输层保护；A10：未经验证的重定向和转发。

5. Web 应用安全联盟(WASC)

Web 应用安全联盟(WASC)是一个组织，它为 World Wide Web 和组成万维网的基于 Web 的软件提供了最佳安全实践标准。这个组织提供了一系列的资源、工具和信息，可以通过它们了解这些基于 Web 的软件开发中常见的安全问题以及如何避免它们。该组织拥有一个 Web 应用程序扫描评估标准，可用于评估各种厂家的产品和实践。它提供了 Web 应用程序的安全指标和威胁分类，并维护着蜜罐进行实时超文本传输协议(HTTP)的 Web 威胁流量分析。这个组织阐述的最常见的顶级攻击方法有：

①跨站请求伪造（CSRF）；②跨站攻击（XSS）；③拒绝服务攻击（DOS）；

④已知漏洞；⑤暴力攻击；⑥隐藏参数操作；⑦网银木马；⑧点击劫持。

6.内建安全 Build Security In (BSI)

美国国土安全部(DHS)提供的最佳实践、工具、指南、规则、原则和其他资源，软件开发人员、架构师和安全从业者可以在开发的每一个阶段用它们把安全整合到软件中。DHS 最初被称为 Build Security In(BSI)，它与其他提到的组织一起协同工作，使整个行业的许多单位可以参与其中并提供有用的材料。美国国土安全部(DHS)有一个软件保障计划来维护 BSI。

BSI 提供了一个与过程无关的方法，可用它处理需求、架构和设计、编码、测试、系统、管理及基本原则。这个成果和 MITRE 公司创始的常见缺陷列表(CWE)紧密结合在一起，常见缺陷列表 CWE 维护了最危险的顶级软件错误。

7.ISO/IEC 27034

ISO/IEC 也制定了关于软件开发的标准。ISO/IEC 27034 标准包括以下条目：应用安全综述和概念、组织规范框架、应用程序安全管理过程、应用安全验证以及特定应用的安全指南。它是 ISO/IEC 27000 系列的一部分，它能让安全的软件开发过程与 ISO/IEC 的信息安全管理体系(ISMS)模型相一致。

8.标准选择

上面列举了网络通信的标准、Web 安全的标准，还有软件开发的标准，各有优长。哪个“最佳实践”或标准最适合你的呢?大多数标准是足以通用于不同的组织和各种软件开发过程，但每一种方法都有其特定的关注重点。CMMI（能力成熟度模型集成）是个过程改进模型；WASC 和 OWASP 的重点是将安全集成到网络软件开发过程中；BSI 重点是保护关键基础设施，但也可以用于任何软件开发项目，而 ISO/IEC-27034 是一个通用性的做法，多使用在单独的行业中。

与大多数技术标准一样，它们之间有很多重合之处。

G.评估和减缓移动系统的脆弱性

主要是安全意识方面了，要有好的习惯什么的。由个人所拥有的设备可使用和应用任何以下术语：便携式设备、移动设备、个人移动设备(PMD)、个人电子设备或便携式电子设备(PED)和个人拥有的设备(POD)。

1.设备安全

①笔记本电脑等设备最好全系统加密，以防被盗。

②手机等重要设备丢失，最好能远程擦除或毁钥什么的。

③离开要锁屏，多次密码错误要锁机。还有好多好多，不写了。

2.应用安全

①密钥要管好，最好有 TPM 芯片。还有什么无所谓了。

3.安全对策

①全设备加密

如果一个设备上的存储媒休都可以被加密，这将是一个有价值的功能。然而，加密不是对数据的保护的保证，特别是如果设备被盗，系统本身有一个已知的后门攻击漏洞。

移动设备使用 IP 语音(VoIP)服务时可以使用语音加密。

②远程擦除

如果一个设备丢失或被盗、远程擦除或远程清除就成为一种常见的措施。擦除过程可以通过移动电话服务或互联网连接进行触发。然而，远程擦除也不是数据安全性的保证。小偷只要不让设备联网就行了。

③锁定

当用户未能提供他们的凭据并多次重复尝试后，帐户或设备被禁用(锁定在一段时间内〉或直到管理员清除锁定标志。

④锁屏

锁屏是为了防止有人随便拾起并能使用你的手机或移动设备。如果黑客通过蓝牙、无线或 USB 电缆等方式连接到设备上，屏幕锁不一定真的能保护设备。

⑤GPS 跟踪

⑥应用控制（强制安装安全软件）

⑦存储分隔（隔离操作系统、应用数据、用户数据）

⑧资产跟踪；⑨库存控制；⑩移动设备管理 MDM；⑾数据访问控制；⑿可移动存储

⒀关闭不使用的功能。

3.BYOD 自带设备（Bring Your Own Device）

BYOD是一项政策，允许员工在工作携带自己的个人移动设备并使用这些设备连接(或通过)公司网络业务资源和/或互联网。虽然 BYOD 可以提高员工的士气和工作满意度，但它增加了组织的安全风险。如果 BYOD 策略是开放式的，则任何设备可以连接到公司网络。并不是所有的移动设备都有安全功能，因此这样的策略不符合设备连上生产网络的标准。一个 BYOD 策略应强制要求特定的设备以减少这种风险，但它可能会要求公司为那些无法购买自有兼容设备的员

工购买设备。

①数据所有权。个人数据和业务数据要分开、隔离。

②所有权支持。明确移动设备坏了谁修。

③补丁管理。定义个人移动设备的补丁管理方法和机制。

④反病毒管理。规定反病毒、反恶意以及反间谍扫描软件是否要在移动设备上安装。

⑤取证。BYOD 策略应该解决相关移动设备的取证和调查。

⑥隐私。ßYOD 策略应该解决隐私和监控。

还有：遵守公司策略、用户接受、架构/基础设施考虑、法律问题、.可接受策略、内置摄像头/视频等等。

H. 评估和减缓嵌入式设备和网络物理系统的脆弱性（例如：可启用网络设备、物联网（LoT））

1. 嵌入式系统安全

①网络隔离。还有好多，反正不考，考了也很容易。

2. 物联网安全

网络化物理系统(CPS)是嵌入有传感器、处理器和致动器的智能联网系统，在设计上可以感知物理世界(包括人类用户)并与其交互，支持安全关键应用的实时和有保障运转。基于 CPS 的架构面临着多种挑战，其中有两个是需要安全专业人员和架构师特别关注的：

*网络安全；*互操作性。

I. 应用密码学

实现安全的重要方法手段，号称是信息安全的基石。不考具体的算法，考是的怎么应用好密码学，每次考个 10 几题。

一、密码学的发展史

1. 早期（人工）时代

凯撒密码/替代密码：已知最早的一种密码系统。朱利叶斯凯撒征服欧洲时在罗马与西塞罗通信时所使用的密码系统。它简单地将字母表中的每个字母都替换为其后的第三个字母，被称 C3 密码。另一种替代密码是 ROT13（字母移动 13 个位置）。

2. 机械时代

①Enigma 的商业编码机：二战德国使用。使用三到六个转子实现了一种极复杂的替换密码，加解密要用同原理的编码机才行。相应的，同盟国军方通过代号为 Ultra 的绝密工作，由波兰军方成功地复原了一台 Enigma 原型机。

②一次性密码本 OTP（vernam cipher/one-time pad）：也称为 Vemam 密码，是唯一宣称只要执行得当便不可破解的密码系统。密码本只能使用一次并且必须与明文同长，使用决不可重复。一次性密码本是不可被频率分或许多其他密码攻击手段破解的。

③多表密码/维吉尼晋城密码：这是一种使用多个表（不是一个字母表）的简单替换密码。教材里用这个算法来解释算法、密钥、密钥空间、加密等概念。

3. 现代密码时代

计算机的各种加密算法和很长的密钥。

4.量子密码学

传统密码学基于数学理论加密，而量子密码学则是利用物理学来保护数据安全。量子密码学(也叫量子密钥分配，简称 QKD)构建在量子物理学之上。最重要的理论是非维尔纳·海森堡的不确定原理：一个人不可能无限准确地同时知道一个粒子的位置和动量。具体而言，量子密码学是一组协议、系统和可以用来创建和分配秘密密钥的规程的集合体。量子密码学解决的是密钥分配问题，密钥交换完成后，常规密码算法便可以使用了。量子密码学完善了安全性，因为每当有人试图窃听安全信道内容的时候，这种行动都会干扰光子的流动，很容易被人识别，从而提供了额外的安全。

量子密码学内有两条独有的信道：

①一条信道用来通过单光子光脉冲传输量子密钥材料；

②另一条信道携带所有消息流，其中包括密码协议、加密的用户通信流等等；根据量子物理学原理，当一个光子被观察到时，它的状态已经改变了。

二、密码学的基础概念

1.密码学的目标

①可用性。②机密性。③完整性。

除了上述信息安全的三大核心原则外，密码工具还可提供其他几个好处。

④不可抵赖性。防止接收者篡改消息并诡称消息的原始状态就是如此。只有公钥(或非对称密钥)密码系统才提供不可否认性。

⑤身份认证。主要通过密钥控制实现，因为只有掌握了密钥的人才能加密消息。

⑥访问控制。只有有权访问正确密码密钥的人才能进行访问。

2.术语

①明文：P

②密文：C

③Kerchoff 原则：算法应当公开，但是所有密钥都应当保密。(Auguste Kerckhoff 于 1883 年发表了一篇论文，指出一个密码系统唯一需要保密的部分应当是密钥。他声称算法应当公开，并且断言：如果安全基于过多的秘密，那么就会有更多的脆弱性可供利用。)

④单向函数（One-Way Functions）：不可能逆向运算出原始值的函数。理论上没有，实际上很多，因为人们还没算出破解函数来。

⑤随机数（Nonce）/初始向量（IV）：这是一个与消息长度相同的随机比特串，并且与原始信息相异或。在每次使用相同密钥加密相同的消息时，密文总不一样。

⑥零知识证明（Zero-Knowledge Proof）：不告诉你密码是什么，但是我可以通过开门来证明我拥有这个密码。

⑦分割知识（Split Knowledge）：和职责分离差不多。要得到一个密钥、或者要开一个门，不能让一个系统搞定、或一个人搞定；必须要几个系统或人同时工作才行。避免密钥被轻易篡改。

⑧工作函数/工作因素（Work Function/Work factor），即工作量：工作函数或工作因数

这个概念，用来衡量密码的强度或解密的难度，一般用成本或时间来表示。也就是暴力破解一个密码所需的计算时间。

⑨加密算法的简写。

在一些资料中，你可能会遇到 RC5-w/r/b 或 RC5-32/12/16 这类符号。它是说明算法配置的简略表达形式。

•w=word=分组长度（字长），单位为位，长度可为 16、32 或 64 位。

•r=round=转换轮数，其值介于 0——255 之间。

•b=bit=密钥长度，16 字节为 128 位。

3.逻辑运算

①与，AND，∧

双真才为真，其它为假

②或，OR，∨

有真就是真，双假才是假。

③非，NOT，！，~

取反。

④异或，ExclusiveOR，XOR，⊕。最重要的计算机运算。

不同就是真，相同就是假。

④模，MOD。最重要的密码学运算。

求整除后的余数。

4.什么是密钥

早期密码系统的算法是必须保密的，没什么所谓的密钥；算法一旦公开或被破解，就没任何保密性了。而现代密码系统的算法是全公开的，安全性靠密钥来实现；也就是说各类系统都使用相同原理的“锁”，给不同的用户主体配不同的“钥匙”就行了。密钥就是一长串的字符，长度是 2 的很多次方，很长很长。

密钥聚类（Key Clustering）：使用相同加密算法但不同密钥对同一明文进行加密产生相同密文的情况。这种情况实际减小了密钥空间，从而降低了密码强度。

密码术（cyptograpgy）：通过加密和解密使通信双方对外界隐藏和验证通信信息的技术或科学。AIO 用这个词，其它其它教材叫“密码学”。

密码分析（cryptanalysis）：在不知道加密算法中使用的原始密钥的情况下，把密码转换成明文的和运算。

密码学（cryptology）：研究密码术和密码分析的科学。

三、密码学方法

加密数据有两种主要方法：流方法和块方法。主要也是用在对称加密里的。

1.流密码 stream cipher

逐位执行加密的密码系统叫做基于流密码（分组为 1 位的块密码就是流密码了）。这是最常用在流应用上的一种方法，例如，语音或视频传输无线等效隐私(WEP)使用了流密码 **RC4**。由于存在把加密密钥暴露给攻击者的许多弱点例如弱密钥大小，这种密码被认为不安全。

流密码使用密码流生成器(keystream generator)，就像是“一次性密码本”，它生成的

位流与明文位进行异或，从而产生密文。正确实施流密码的难点在于要生成一个真正随机而平衡的密钥流，一般要用初始化向量 IV 来提高随机性。

2.块密码/分组密码 block cipher

块密码对成块的文本运算。明文在输入密码系统的过程中，被分解成预定大小的块—通常是 ASCⅡ码大小的倍数——64、128、192 位等。一个强密码必须具有两个主要属性：扰乱和扩散，以确保攻击者不可能对其进行逆向工程。**扰乱(confusion)**通常通过替代实现，**扩散(diffusion)**则通过换位实现。密钥值的随机性和数学函数的复杂性也决定了所涉及的扰乱和扩散的级别。大多数块密码结合使用了替代和置换运算。这使块密码相对而言强于大多数基于流密码，但计算密度更大，执行成本往往也更高。也正是由于这个原因，许多基于流密码在硬件中执行，而基于块密码在软件中执行。

①扰乱（混淆）指的是使密钥和密文之间的关系尽可能复杂，从而令攻击者无法从密文中发现密钥。每个密文值都应依赖于密钥的若干部分，但在观察者看来，密钥值和密文值之间的对应关系应当看上去是完全随机的。（算法很复杂）

②扩散（置乱）指的是单独一个明文位会影响到若干密文位。改变一个明文值应当更改许多而不是一个密文值。实际上，在强分组密码中，如果改变一个明文位，那么每一个密文位都会发生变化的几率为 50%。与扩散非常类似的一个概念叫做雪崩效应。如果一个算法非常符合雪崩效应准则，这就意味着算法输入值的轻微变化会引起输出值的显著变化。即密钥或者明文的少量变化会引起密文的显著变化。（结果很多样）

③**SP-network**。为了增强分组加密（块加密）算法的强度，替换 substitution 和置换 permutation 这 2 种方法都要用，反复用，以实现扰乱和扩散，这被称为 SP-network。

在算法中，将一个分组中的各个位打乱或者分散到整个分组内，即可实现扩散。扰乱则通过执行复杂的替代函数来实现，这样坏人就无法了解如何替换正确的值以得到原始的明文消息。假设我有 500 块上面写有字母的木块，将它们排列起来拼出一封电报(明文)。然后，我使用另外 300 块木块替换其中 300 块木块(通过替代实现扰乱)。接下来，我将所有木块打乱(通过换位实现扩散)，并将它们堆成一堆。如果你想要得到原始的消息，那么就必须替换正确的木块，并将它们接正确的顺序排列。这很难做到。

3.初始化向量 IV(Initialization Vector)

IV 是一个随机值，用于确保加密过程中不会产生某种规律性的模式。它们与密钥一同使用，而且在传输时不需要加密。如果不使用 IV，相同明文会得到相同的密文，攻击者可以轻松破解密钥。

4.会话密钥(session key)

会话密钥是只使用一次的对称密钥，用于对通信会话期间两个用户之间的消息进行加密。

5 密码学在网络通信领域的应用

通信线路加密有两份种方式（IPsec 的 EAP 模式也有这 2 种通信方式）：

①链路加密（Link encryption）：建立 1 个安全隧道，所有的数据(包括头、尾、地址和路由数据)被加密，路由每一跳都需要解密再加密转发，速度慢。

③端到端加密（End-to-end encryption）：不加密头、尾、地址和路由数据，速度快，但易遭嗅探和窃听。

端到端加密的一个典型应用是 SSH（Secure Shell）安全外壳。SSH 为 FTP，Telnet,rlogin 等提供加密解决方案，有 2 个版本：

SSH1,不安全,支持 DES, 3DES, IDEA,和 Blowfish 算法；

SSH2，安全，不支持 DES/IDEA,支持其它算法。

6.通信线路加密的一个典型体系结构就是 IPsec

IPSec 是由互联网工程任务组(IETF) 确立的标准体系结构，没规定技术实施的细节，是一个开放的模块化架构，目的是实现实体（系统、路由器、网关、计算机等）之间的通信加密。IPSec 使用公钥密码算法来提供加密、访问控制、不可否认性以及消息身份验证，使用 IP 协议，被广泛应用于虚拟专用网(VPN)。

IPSec 通常与二层隧道协议(L2TP)一起使用，可以工作在两种模式：传输模式或隧道模式。传输模式只有数据包有效载荷被加密，用于对等通信；隧道模式对整个数据包(包括头)都加密，用于网关间通信。IPSec 有 2 个重要的组件：

①身份验证首部(AH)。提供消息完整性和不可否认性，提供身份验证和访问控制，并且可以防止重放攻击。

②封装安全有放载荷(ESP)。提供数据包内容的机密性和完整性。ESP 还提供加密和有限的身份验证，并且可以防止重放攻击。

IPSec 另一个重要概念是安全关联(SA security association)，SA 就是 1 个单向的通信会话，并记录与连接有关的配置和状态信息。双向信道就有 2 个 SA，要同时支持 AH、ESP 就要 4 个 SA。

IPSec 还有很多内容要考，详见第四域 C.4 章节。

7.网络安全关联和密钥管理协议(ISAKMP) The Internet Security Association and Key Management Protocol

ISAKMP 是为 IPSec 提供后台支持的，主要功能是协商、建立、修改、删除和管理安全关联（SA），具备 4 方面的主要能力：

①对通信主体（peer）进行身份验证。

②建立并管理安全关联 SA。

③提供密钥生成机制。

④防止遭受威胁(例如重放和拒绝服务攻击)。

I.1 密码生命周期 （例如：加密的局限性、算法/协议治理）

除了一次一密，所有的密码系统都有一个有限的寿命。一方面，加密的数据是有保密期限的，有的是 1 天，有的是 10 年，到期就可以公开了；另一方面，加密的算法、协议和密钥长度随着技术的发展，很快就会过时，需要与时俱进。

业界一般用“强”、“弱化”和“遭破坏”等词来描述密码系统生命周期的各个阶段。NIST 以下几个词语描述算法和密钥长度的：“可接受”、“不宜使用”、“受限”、“没有用途”。

I.2 加密类型 （例如：对称加密、非对称加密、椭圆曲线加密）

一、对称密钥算法/对称加密/私有密钥/秘密密钥/单钥密码/共享密钥 common key

消息的加密和解密使用相同的密钥，消息的发送者和接收者都要拥有这个密钥才行。凯撒密码、斯巴达密码棒和恩尼格玛密码机等算法和系统都是对称算法的例子。接收者需要用加密流程中使用过的同一个密钥来执行解密流程。

先解释一下“私钥”这个概念：

在对称密钥算法中，“私钥”指是的私有密钥密码学或公钥密码学，也就是对称加密的意思，它的字面涵义是指收、发双方都要保守这个秘密（相同的密钥）。

在非对称密钥算法中，即所谓的公钥密码学，“私钥”是与“公钥”相对应的概念，是这个密钥对中不公开给其它通信对象的密钥，它的字面涵义是指收、发双方仅要保守自己的这个秘密（独有的私钥）就行了，不关其它人的事。

对称密码学运算很快，简单高效，可以集成到硬件里，但缺点是很明显的（考点）：

①可扩展性差。它不能用于大量用户间的加密，因为每一对不同用户间的点对点通信加密都要一个密钥，这个量很大，管理和分发这些密钥也很麻烦。N 个对象间要 N×（N-1）/2 个不同的密钥。

②密钥必须经常更新。如果 1 个人离职，不使用加密系统了，整个系统的密钥都要换掉，不然就不安全了；就算没人走，也要经常换换，怕有人泄露密钥；而且分发密钥必须通过带外安全途径。

③不能实现不可否认性（抗抵赖性）。使用同一密钥的多个通信对象间，无法证实该消息是由确认的某个对象发出来的，它不提供数字签名之类的功能。

下面是必须熟悉的对称加密算法：

1.数据加密标准（DES）Data Encryption Standard

DES 是一种算法标准，DEA 是其具体实现，两个概念可以混用。美国 1977 年搞的 DES 已经过时了，但它很精典，一直被优化升级。基本原理：明文按 64 位的长度逐段拆分，用 64 位的字串来逐段异或（XOR），于是得到了密文。记住几个概念：

DES 的分组长度是 64 位，密钥是 **56 位**！64 位字串中有 8 位是奇偶信息，不是密钥。加密、解密要异或 16 次，1 次被称为是 1 轮（round），DES 为什么是 16 轮转换呢，开发者就这么定的，他觉得这个够安全了，算的也快。不过可以很快被暴力破解。

下面是 DES 的 5 种操作模式（必考），也就是分组加密/块加密的方式：

前 2 种是在块结构中运行的；后 3 种是在流模式中运行的。

①电子代码本模式（ECB）Electronic Codebook Mode，照本宣科

ECB 简单容易不安全，就是每个 64 字串都用相同密钥来运算，毫无变化。相同的明文会得到相同的密文。搞得多了，破密者就可以搞出 64 位字串的明、密对照代码本了，不要密钥也能解密。

这个脆弱性使得 ECB 仅能用于短代码的加密传输，用它来做主用通信加密手段并不现实（因为长文本很容易被破密者归纳出明、密对照的代码本）。

②密码分组链接模式（CBC）Cipher Block Chaining Mode，逐串变化

先用 1 个 64 位 **IV**（初始向量）来异或变换明文的第 1 个分组，再做 16 轮加密变换；后续的分组都要用上一组的密文来先变换明文，再加密。这样相同明文不可能得到相同的密文。CBC 用的 IV 可以明传给对方，也可以密传给对方。不过，如果加密过程中或传输过程中丢失

了一些字串，就不可能再解密了，环环相扣啊。

③密码反馈模式（CFB）Cipher Feedback Mode，实时的逐串变化

CFB 就是 CBC，也用 IV 和链接，只是运算的方法不一样。（也有说 CFB 对 IV 加密了）

链接模式 CBC 在硬盘里算，把明文拆分，用 IV 逐个算出密文，明文、密文都存在硬盘上；

回馈模式 CFB 在内存里算，直接边算边发送，不用硬盘，它读明文的第 1 组 64 位，算完发出去，接着读第 2 组，用上一组密文转换后再加密，接着发出去。因为算的很快，完全就是个数据流。

CBC 就相当于是笔译，记下来翻译；CFB 就相当于同声翻译，边听边说，直接大脑反应。

④输出反馈模式（OFB）Output Feedback Mode，容错的逐串变化（用的最多）

OFB 就是 CFB,用 IV,运算方法一样，只是每个字串的明文变换不依赖上一个字串，而是通过 IV 为每组字串都计算出一个种子值（seed value），再用这个种子值与对应字串做异或运算，得到变换的明文后再加密。

输出回馈 OFB 在内存里算，因为 IV 是可以明传的，所以就算中间有丢包，也可以通过 IV、密钥和字串序号来解密；但 CBC 和 CFB 的消息内容是密传的，每组字串的加密和解密都要依赖上一组密文，一旦中间少了几串，就无法得知变换的 IV 到底是什么了，也就无法解密。

⑤计数模式（CTR）Counter Mode，更快的容错的逐串变化

CTR 就是 OFB，用种子值的流密码运算，不过种子值不依赖上一个种子值，而是直接通过字串的序号和 IV 来算出对应的种子值。这样算起来更快了，不用从第一个种子值一路推算到第 N 个种子值，可以直接根据序号算出种子值来，好处是长文本的加密可以被拆分成很多个小文来进行并行运算。CTR 用于 IPsec 和 ATM 等。

总结一下：懒得写了，自己归纳 5 种模式的特点吧，第 5 种是最好的。

2.三重数据加密算法(3DES) Triple DES

DES 的 16 轮变换和 56 位密钥不够安全，现在计算机速度这么快，早就可以很快破解了。完成可以再多变换几轮，可以用 2 到 3 个密钥甚至更多的密钥来搞好几个 DES 来回变换，把机器都转晕了。这里要了解 4 种 3 重 DES 的方法：

E 代表 1 次 16 轮的 DES 加密；数字代表密钥的个数；P 代表明文；C 代表密文；E(K,P)代表用密钥 K 对 P 进行加密；D 代表解密。

①DES-EEE3，C=E（K1,E（K2，E(K3，P)））,有效密钥=56×3＝168 位。看不懂就换个方式表达：EEE3 就是用 3 个密钥分别加密 3 次。

②DES-EDE3，C=E（K1,D（K2，E(K3，P)）），与①一样，第二次是解密，不是加密。

③DES-EEE2，C=E（K1,E（K2，E(K1，P)）），与①一样，只用 2 个密钥，共 112 位。

④DES-EDE2，C=E（K1,D（K2，E(K1，P)）），与②一样，第二次解密，用 2 个密钥。

为什么用三重而不是两重 DES 呢，因为两重的加密强度与一重相比并没有提升（通过使用中间相遇攻击）。

3.国际数据加密算法(IDEA) International Data Encryption Algorithm

IDEA 的算法和 DES 是一样的，只是扩充了密钥的长度。它对 64 位字串进行异或（XOR）和求模（MOD）操作，将 128 位密钥分解成 52 个 16 位密钥来用，可以使用 DES 的前四种转换模式（分组加密运算方式），不能使用 CTR 模式。IDEA 最重要的应用就是 PGP（可靠隐私安全

电子邮件系统）。

PGP（Pretty Good Privacy）有两版本：商业版本使用 RSA 进行密钥交换，使用 IDEA 进行加密/解密，使用 MD5 生成消息摘要；免费版本则使用 Diffie-Hellman 进行密钥交换，使用 Carlisle Adams/Stafford Tavares (CAST) 128 位算法进行加密/解密，使用 SHA-1 生成消息摘要。

4.Blowfish

Blowfish 比 IDEA 和 DES 更快，也是 64 位变换，还扩展了密钥的强度和灵活性，密钥长度从 32 位到 448 位可变。它是公开免费的算法，用在 LINUX，美国政府没选择用它来代替 DES。

5.Skipjack

美国政府搞的 DES 算法，也是 64 位变换，但使用一个 80 位的密钥。

它支持并集成到 Clipper 和 Capstone 高速加密芯片中；最可怕的是它支持密钥托管，NIST 和财政部各管部分代码，在法律允许的情况下，美国政府可以随意解密。所以除了政府强制，没人喜欢用它。

6.RC5 密码 Rivest Cipher 5

RC4 是对称加密，它更是一种流密码。RC4 算法本质上是一个由最长 256 密钥初始化的伪随机数发生器（PRNG），其产生的密钥流与明文进行异或。它速度是最快的，但效率低，很快被破解了，无线的 WEP 加密就用了它。它密钥长度可变，现在用于 SSL。

RC5 是 RSA 数据安全公司的商秘算法，收费的。RC5 就不是固定的对 64 位字串进行变换了，它支持可变的字串长度（32、64、128 位）和可变的密钥长度（0-2048 位）和可选的加密轮数（最多 255 轮）。

7.高级加密标准(AES) Advanced Encryption Standard

2000 年，美国总算搞出来 DES 的升级替代算法了，基于 Rijndael 算法。它采用密码块链接消息认证码协议(CCMP)的计数器模式。商业部要求所有非政府的密级信息要用这个来加密，它的特点就是有 3 种密钥长度和加密强度：

128 位密钥进行 10 轮加密；192 位 12 轮；256 位 14 轮（40 年可破）。

身为加密协议的 CCMP 是 802.11i 无线局域网标准的一个组成部分。CCMP 协议基于 AES，其中 CRT 模式是它的加密算法。CBC-MAC(CCM)模式则用于消息完整性运算。

CCMP 中的 AES 处理必须使用 AES 128 位密钥、128 位数据块（分组）和一个 48 位的初始向量 IV，且根据美国联邦信息处理标准，AES 算法(一种块密码)使用大小为 128 位的块，长度为 128、192 和 256 位的密码密钥，运算轮数相对为 10、12 和 14 轮，CCMP 使用了 128 位密钥和一个 48 位 IV，可以最大限度减少面对重放攻击的脆弱性。CTR 成分可以提供数据隐私保护。密码块链接消息认证码成分产生了个消息完整性代码可为数据包有效载荷数据提供数据源认证和数据完整性保护。802.11i 标准包含 CCMP。AES 常被 802.11i 称作加密协议，但 AES 本身其实只是个块密码，加密协议实际上是 CCMP。

8.Twofish 算法/双鱼-2 个 64 位

Twofish 是另一种 AES ，处理 128 位的字串分组，使用最大 256 位的密钥。

Twofish 用了两种新技术：预白噪声化和后白噪声化（Prewhitening，Postwhitening），是指用一个独立不同的子密钥来对文本进行变换，提高随机性；预白就是先对明文洗白白，后

白就是对最后的密文再洗白白。

总结：每种算法的字串分组长度和密钥长度是多少位、可不可变要自己去归纳记忆，虽然书上有表格，自己不弄，记得不牢。

9.对称密钥的管理/密钥的带外分配

最后要讲一下对称加密最麻烦的事了：分发和管理密钥！

密钥的管理实践包括：密钥的生成、分发、存储、销毁、恢复和托管。其中：

存储密钥要注意两个问题：一是密钥别跟加密的数据存在一起，要另外保管；二是密钥别完整的存储，要分给 2 个人各保管一半，这就是知识分离原则（split knowledge）（考点）。

10.密钥分配中心(KDC)

在 Kerberos 系统中，详见第五域 B.1 章节，用密钥分配中心 KDC 来管理密钥：

①第一种是主密钥，这是由每个用户和 KDC 共享的私钥。每个用户都有自己的主密钥，用于加密用户与 KDC 之间的通信流。

②第二种密钥是会话密钥，在需要时创建，在通信会话期间使用，会话结束后废弃。

11.密钥分发

重点讲对称密钥的 3 种分发方法：

①离线分发（Offline Distribution）

就是机要部门经常要干的注钥、换钥工作，将密钥载体通过物理连接直接注入到保密系统或设备中；最大的缺陷就是密钥在运输过程中可能被截获。

②公钥加密（Public Key Encryption）

许多通信者希望充分利用对称加密算法的速度优势，同时又能克服密钥分发过程中存在的安全缺陷。方法就是：用公钥算法来验证身份、建立初始通信连接，并传送密钥；用私钥算法来传送大量数据。一般情况下，私钥加密的速度比公钥快 1000 倍。

③Diffie-Hellman 算法（非对称加密算法）

如果没有可靠的运输途径，没有合适的公钥基础架构，前面 2 种方法都不行。

Diffie-Hellman 算法就是密钥交换算法，它是非对称加密，基于离散对数难题 Discrete logarithms，也称为指数密钥协商 Exponential Key Agreement。它的基础是收发双方已经约定了两个很大很大的，独有的，相当于密钥作用的数字；然后就可以放心的交换对称密钥了。它的基本流程如下：

1.收发双方约定好 2 个很大很大的数字：质数 p 和整数 g，其中 1<g<p。

2.发方自己选一个随机的很大的整数 r；算出一个大 R，$R=(g^r)$ MOD p。

3.收方自己选一个随机的很大的整数 s；算出一个在 S，$S=(g^s)$ MOD p。

4.收发双方互换大 R 和大 S。

5.发方算出密钥 $K=(S^r)$ MOD p；

6.收方算出密钥 $K=(R^s)$ MOD p。

为什么两 K 算出来是一样的，我也没搞清楚。反正 K 就可以用作对称密钥了。

这个算法仅用于密钥协商即安全的发送密钥，并不提供数据加密和数字签名的功能。

二、非对称密钥算法/公钥密码学 Asymmetric Key Cryptography/Public Key

每个人有 2 个密钥，称之为密钥对，即一个公钥、一个私钥；公钥是公开共享的，私钥是自己独有的，加密和解密必须是一个公、一个私，或者一个私、一个公。这样解决了对称加密算法的很多不足，带来的优点有：

①随意扩展。有多少用户，就需要多少对密钥，这个量是很少的，也好管理，人再多也不怕。

②密钥不用经常更新。每个人保护好自己的私钥就行了，如果离职了，就删除自己的密钥，不影响其它人的加密，也不用换掉全部的密钥。密钥的分发管理也很简单，带内发送就行。

③实现了不可否认性，还有完整性和身份验证。私钥还可以这么用：先对要发送的消息进行散列运算（MD5 什么的），得到 1 个消息摘要；再用私钥对这个消息摘要进行加密，得到 1 个数字签名；然后把加密的消息、数字签名和公钥都发出去就行了；最后，接收者用它的公钥解密消息得到消息明文，用公钥解密数字签名得到消息摘要明文，用散列运算得到接收文件的消息摘要，对比一下消息摘要（散列值）是否一致，就知道这个消息是不是可靠的了。这里面，消息摘要提供了完整性；数字签名提供了身份验证，也就是不可否认性。

对发送方来说，如果机密性很重要，那么他就会使用接收方的公钥来加密文件。因为只有拥有相应私钥的人才能进行解密，这称为安全消息格式(secure message format)。

对发送方来说，如果身份验证很重要，那么他会使用自己的私钥来加密数据。这保证了只有拥有该私钥的人才能加密这些数据，这称为公开消息格式(open message format)。

非对称加密最大的缺点就是运算很慢啊。如果要对大量的传输数据进行加密，最好结合两份种方法：用非对称系统来建立通信连接，给对方发送 1 个对称系统用的共享密钥；再用对称系统来加密随后进行的大数据通信。同时使用这两种技术称为混合方法（混合加密），也经常被称为数字信封(digital envelope)。

下面是几典型的公钥算法：

1.RSA

最著名的、商业的公钥加密系统。基本原理是：大质数的因数分解很难很难，质数就是素数。它的密钥对是这么算来的：

1.选 2 个很大很在的质数（200 位以上，比密钥还长）p 和 q，算出其乘积 n=p*q。

2.找出合适的数 e 和 d 分别用来生成公钥和私钥，其中：

①e<n，且 e 与(n-1)*(q-1)互质；

②d 满足(e*d-1) MOD (p-1)(q-1)=0

3.e 和 n 共同作为公钥，d 作为私钥；加解密过程如下：

$C=P^e$ MOD n

$P=C^d$ MOD n

安全多用途互联网邮件扩展(S/MIME) 协议就使用 RSA 加密算法，并依靠 X.509 证书交换密钥。S/MIME 还支持 AES 和 3DES 对称加密算法。它目前主要应用于桌面邮件应用程序，并没用在 Web 电子邮件系统。(需要浏览器插件)。RSA 加密速度很慢，密钥长度一般为 2048 位。

攻击 RSA 算法的三种主要方法是：

①蛮力攻击，尝试所有可能的私钥。

②数学攻击，因子分解两个质数的乘积。

③T 计时攻击，计量解密算法的运行时间。

2.背包算法 Merkle-Hellman / Merkle-Hellman Knapsack

与 RSA 一样，这种算法也基于因式分解操作的困难性，但是它依赖于被称为**超增序列**的集合论组件，而不是依赖于大质数。它在 1984 年被破解了。

3. El Gamal 算法

对称密码中的 Diffie-Hellman 算法使用大的整数和模数算法来安全交换私钥。1985 年，T.EI Garnal 博士利用这个原则开发了非对称密钥算法。它是公共免费的，不是商业收费的。不过它最大的缺点是加密的密文长度比明文增加了 1 倍，如果是窄带传输大数据，这个算法显然不适用。

4.椭圆曲线密码系统(ECC) Elliptic Curve Cryptosystem

ECC 肯定会考的，它的数学原理很复杂，其基础是椭圆曲线的离散对数问题（ECDLP），它比 RSA 的质数因数分解、以及 Diffie-Hellman 与 EI Gamal 的标准离散对数还要难。不过不用了解那么细，知道大概就行了。记住 1024 位的 RSA 密钥强度相当于 160 位的椭圆曲线密钥强度！它的速度明显比 RSA 快得多。

5.非对称密钥的管理

对称密钥分发很麻烦，那非对称密钥呢，不用操心怎么分发的，只要管好生成与使用环节就行了。主要做法：选择公开的加密算法；确保密钥完成随机生成；选择合适的密钥长度；个人必须管好自己的私钥；定期换钥；安全备份密钥。

I.3 公钥基础设施（PKI）

公钥加密系统的 1 个主要优点是可以验证对方的身份，使陌生双方之间的通信更可靠。

而受信任的公钥基础设施(PKI)是实现公钥加密系统的基本条件，它一般结合了非对称和对称算法以及哈希（散列函数）和数字证书。很像公安制证中心管身份证。PKl 提供下列安全服务：•机密性；•访问控制；完整性；•身份验证；•不可否认性。

1.证书 Certificates

数字证书（Certificates）不是数字签名（digital signature）。

数字签名可以证明 1 个信息是属于某个密钥对的；

数字证书可以证明这个密钥对是属于某个真实的人或机构的。

怎么证明呢？必须要有一个可信的**证书颁发机构（CA）**Certificate Authority 来发布被认可的证书；你要想拥有证书，就必须带一堆资料去 CA 做实名验证和登记，这样 CA 才发布证书来代表真实唯一的你。

数字证书的国际标准是 **X.509**（X.500 电子目录服务系列标准中的），它用在了 SSL 中，它规定数字证书的数据包括以下内容：

①X.509 版本号；②序列号（CA 编号）；③签名算法标识符；④发布者（CA）；⑤有效期；⑥证书主体（持有人的唯一名字）；⑦主体的公钥。

这里插播一下 SSL：

安全套接字(SSL) Secure Sockets Layer 和安全传输层协议(TLS) Transport Layer Security(必考)

SSL 协议对访问网站的流量进行加密，使用 HTTPS 协议和 443 端口，实施过程如下：

①当用户访问网站时，通过浏览器检索 Web 服务器的证书，提取出服务器的公钥。

②浏览器创建一个随机的对称密钥，使用服务器的公钥来加密，并发送给服务器。

③服务器用自己的私钥解密得到对称密钥，然后双方使用对称密钥来实现加密通信。

而 TLS 则作为 SSL 标准的升级和替换，也使用 TCP 端口 443，由于误解，TLS 也被称为 SSL 3.1 版本，其实它和 SSL3.0 版不一样，也不再向下兼容了。详细内容在第四域的 C 和 C.3 章节都有。

下面是一些主要的证书授权机构 CA，不考，简单了解下吧：

赛门铁克 Symantec，Thawte，GeoTrust，GlobalSign，Comodo Limited，Starfield Technologies，GoDaddy，DigiCert，Network Solutions，LLC，Entrust

证书仅代表了 CA 是认可该主体的，现在已经有很多 CA 被拉黑名单了，因为他的证书花钱就能买，乱搞。数字证书光有 CA（Certificate Authorities）生成并发布是不够的，证书要在 CA 的数据库里注册了才有效，使用它的系统和人也要对遇到的各种证书进行验证才行，这就用到了 RA（Registration Authorities）。CA 就是给你发本本的机构，RA 就是登记这个本本相关信息的服务器。当其它系统要验证你时，就会上 RA 核对下你的证书本本。

证书路径确认（CPV）Certificate Path Validation（考点）

CPV 指的是：证书链上的所有证书都是合法有效的，这个证书链包括从 CA 到 RA、服务器到客户端、系统环境到三方系统的所有相关的证书。其中任一证书过期或被替换时，必须重新验证整个证书链。证书是否过期，是否有效可以通过 2 种方式来核对证书撤销列表（CRLs，Certificate Revocation Lists）：

证书的撤销都是 CA 要做的事，如果撤销了，就要通知大家：一是定期下载 CRLs；二是通过联机证书状态协议(OCSP) The Online Certificate Status Protocol 实时验证。后者效率更高，自动更新。

2.注册授权机构 RA

RA 执行证书注册任务。RA 建立和确认个人的身份，代表终端用户启动使用 CA 的认证过程，以及执行证书生命周期管理功能。RA 不能发行证书，但是可以作为用户和 CA 之间的中间人。当需要新证书的时候..用户就会向 RA 发送请求，然后 RA 再将该请求发送给 CA。

3. PKI 步骤

①终端用户注册自己，即获取一个数字证书的过程：

(1)用户向 RA 发送一个请求。

(2)RA 向他索取特定的身份标识信息，如驾驶执照副本、电话号码、地址等。

(3)RA 接收并验证其身份标识信息，通过了就将用户的认证请求发送给 CA。

(4)CA 创建一个证书，该证书嵌入了用户的公钥及其身份信息(私钥/公钥对由 CA 或用户的计算机在本地创建，这取决于系统的配置。如果由 CA 创建，那么就要通过安全的方式将私钥发送给用户。在大多数情况下，用户会生成这个密钥对，然后在注册过程中发送他的公钥)。

②终端用户与其它用户保密通信的过程：

(5)用户从一个公共目录请求得到对方的公钥。

(6)这个目录(有时也称为存储库)将对方的公钥发送给用户。

(7)用户验证数字证书并提取对方的公钥，并使用该公钥加密一个会话密钥，这个会话密钥将用于加密他们之间传递的消息。然后将加密的会话密钥发送给对方，还要将自己的、包含其公钥的证书也发送给对方。

(8)对方接收到用户的证书时，其浏览器会询问 CA 是否对该证书进行了数字签名。只有对方的浏览器信任这个 CA，并且验证了证书，双方就可以进行加密通信了。

I.4 密钥管理实践

其实就是口令/密码管理。密钥的大小以及密钥的保密是实现密码系统安全的核心两个要素。对称与非对称密钥的管理在上一章都讲过了。这里讲点别的：

1.XML 密钥管理规范 2.0（XKMS）

XKMS 规范定义了分配和注册公钥的协议，适合于与 XML 数字签名和 XML 加密配套使用。

2.金融机构的标准

ANSI X9.17 标准用于金融机构的安全传输，特别描述了确保密钥保密性的手段。

3.职责分离

密钥不能一个人管，必须分开来。对于小公司，人员很少，可以采用其他补偿控制来达到同样的控制目标，如：活动监测、审计跟踪和管理监督等。实现职责分离有 2 个重要机制：双重控制和分割知识/知识分离。

①双重控制 dual control。2 个或多人要同时一起来完成一个流程。（2 人同控）

②知识分离 split knowledge。密钥或资产要分发给不同的人来保管。（2 人分管）

4.密钥强度

RSA 数据安全公司指出：

1024 位 RSA 密钥等于 80 位对称密钥、

2048 位 RSA 密钥等于 112 位对称密钥、

3072 位 RSA 密钥等于 128 位对称密钥，2048 位密钥在 2030 年之前是够用的。

此外，1024 位的 RSA 密钥强度相当于 160 位的椭圆曲线密钥强度。

5.密钥丢了怎么办？

M-N 方法：如果密钥涉及到 N 个人的利益，要想找回，必须要同时有最少 M 个人来操作。

M of N Control requires that a minimum number of agents (M) out of the total number of agents (N) work together to perform high - security tasks.

I.5 数字签名/（MAC）

公钥密码系统加上散列函数，就可以用来做数字签名了，数字签名要实现 2 个主要目标：

①确实证明了发送者的身份，具有不可否认性。（不可伪造）

②确实证明了消息没有改变，实现消息完整性。（没有篡改）

I.2 的第二大点：非对称密钥学里已经讲过签名流程了，这里再描述一遍：

先对要发送的消息进行散列运算（SHA-512 什么的），得到 1 个消息摘要；再用私钥对这个消息摘要进行加密，得到 1 个数字签名；然后把加密的消息、数字签名和公钥都发出去就行了；最后，接收者用自己的公钥解密消息得到消息明文，用对方公钥解密数字签名得到消息摘

要明文，用散列运算得到接收文件的消息摘要，对比一下消息摘要（散列值）是否一致，就知道这个消息是不是可靠的了。这里面，消息摘要提供了完整性；数字签名提供了身份验证，也就是不可否认性。

这个过程也可以把消息明文发送出去，只加密消息摘要就行了，这样提供了身份验证，但并没有保护信息隐私。数字签名也常用于软件下载分发、驱动程序什么的。

1.消息验证码/消息身份认证码(MAC) Message Authentication Code/（保护完整性）

消息验证码和散列函数（哈希）差不多，只不过多了身份认证和加密，可以防止被伪造。

为了防范中间人攻击，需要使用消息身份验证码 MAC，它对消息发送者的身份进行验证，并不是对消息进行加密。MAC(亦称密码校验和)是用秘密密钥（对称加密）生成的一小块数据，附着在消息上。当消息被接收时，接收者可以用私钥生成自己的 MAC，从而得以知道消息在传输过程中是否曾被无意或有意改动过。MAC 这个词还有另外两个意思：强制身份认证、MAC 地址。这里 MAC 有 3 种基本类型：

①散列信息身份验证代码(HMAC) Hashed Message Authentication Code

使用散列和共享密钥，验证完整性，提供数据源身份验证。

②CBC-MAC。提供完整性验证、数据源身份验证，但是不提供机密性，并不加密数据。

③CMAC。就是 CBC-MAC 的升级版，还是不加密数据，更复杂更安全。

也有分成 4 种类型的：

①无条件安全消息认证码 unconditionally secure MAC。基于一次一密本或一次性密钥。

②基于散列函数的消息认证码 hash function-based MAC,HMAC。基于散列函数。

③基于流密码的消息认证码 stream cipher-based MAC。基于流密码和线性反馈移位寄存器 linear feedback shift registers,LFSRs 。

④基于分组密码的消息认证码 block cipher-based MAC。将分组密码（DES-CBC）得到的最后密文分组做为消息认证码。

散列、HMAC/CBC-MAC 和 CMAC

MAC 与散列过程可能容易令人混淆。表 7-2 简要说明了它们之间的差异。

表 7-2　MAC 与散列过程的区别

函　数	步　骤	提供的安全服务
散列	(1) 发送方使用散列算法处理一条消息，生成一个消息摘要(Message Digest，MD)值 (2) 发送方将消息和 MD 值发送给接收方 (3) 接收方使用相同的散列算法处理消息，并创建一个独立的 MD 值 (4) 接收方比较这两个 MD 值。如果两者相同，那么就表示消息未被修改	完整性。不提供机密性或身份验证，只能检测无意的更改
HMAC	(1) 发送方将合并消息与秘密密钥，并使用散列算法处理得到的结果，从而创建一个 MAC 值 (2) 发送方将 MAC 值附加在消息后，并将其发送给接收方 (3) 接收方在消息后合并自己的对称密钥，得到一个独立的 MAC 值 (4) 接收方比较这两个 MAC 值。如果两者相同，那么就表示消息未被修改。同时，接收方知道消息来自哪个系统	完整性和数据源身份验证。不提供机密性
CBC-MAC	(1) 发送方在 CBC 模式下使用对称分组算法来加密消息 (2) 最后一个分组用作为 MAC (3) 明文消息和附加的 MAC 发送给接收方 (4) 接收方加密收到的消息，创建一个新的 MAC，并比较两个 MAC 值。如果两者相同，那么就表示消息未被修改，并且接收方知道数据来自哪个系统	数据源身份验证和完整性。不提供机密性
CMAC	CMAC 的工作方式与 CBC-MAC 相同，但是基于更复杂的逻辑和数学函数	

2.正确使用密钥

*加密消息，使用接收者的公钥。

*解密消息，使用你自己的私钥。

*生成数字签名，用你自己的私钥。

*验证数字签名，用发送者的公钥。

3.数字签名标准（DSS）Digital Signature Standard

数字签名是指用户用自己的私钥对原始数据的哈希摘要（散列值）进行加密等到的数据。接收者通过用对方的公钥解密数字签名，再对照原文的哈希值，就能实现完整性和身份验证（不可抵赖性）了。

美国国家标准和技术协会在联邦信息处理标准(FIPS) 186-4 中指定了联邦政府可以使用的数字签名算法，该标准也被称为数字签名标准(DSS)。标准规定美国政府的所有数字签名算法都必须使用 SHA-2 散列函数；数字签名基础结构的加密算法可以三选一：

①数字签名算法(DSA)，在(FIPS) 186-4 中指定。

②RSA 算法，在 ANSIX 9.31 中指定。

③椭圆曲线 DSA(ECDSA) ，在 ANSIX 9.62 中指定。

还有 2 种算法政府没认可，不过也要了解下：

Schnorr’s 和 Nyberg-Rueppel’s 的签名算法。

I.6 数字版权管理（DRM）

内嵌的标志或商标称为数字水印(digital watennark)。不同于将秘密消息嵌入图形以期望不被发现，数字水印往往是可以看见的。数字水印的作用是阻止人们使用其他人的素材。这种隐写术称为数字权利管理 DRM(Digital Righs Management)，其目标是限制使用某家公司或个人所拥有的素材。

1.隐写术和水印 Steganography and Watermarking

隐写术是使用密码学技术在另外一个消息内嵌入秘密消息的方法。通常做法：修改图像数据中最不重要的数据比特，并不影响图像的浏览。隐写术也被用来做文档的水印。

I.7 抗抵赖

不可否认性/不可抵赖性/可问责性确保发送者无法否认自己发送了一条消息且消息的完整性是原封不动的。不可抵赖性可通过数字签名和 PKI 实现。具体前面都讲了。

I.8 完整性（哈希法和加盐法）/散列

散列不是加密，是单向的数据转换，是把很长的消息转换成独一无二的一个很短的消息摘要，这个摘要无法还原成消息的，就是用来验证消息是不是被篡改了，也用于实现数字签名。

术语“消息摘要”也被称为：散列、散列值、散列总数、CRC、指纹、校验和和数字 ID 等，英文为：message digest 以及 hash,hash value,hash total,CRC,fingerprint,checksum,and digital ID。

消息摘要通常为 128 位，当然，数值越长，完整性验证就越可靠。按照 RSA 公司的标准，散列函数应具备以下条件：

①广泛性：输入入值可以是任意长度。

②确定性：输出值具有固定的长度，原文不变，散列就不变。

③均匀性：散列计算容易实现，且不可预测。

④难逆向：散列计算是单向的(无法)。

⑤抗冲突/抗碰撞：散列值是唯一的(不同消息必须算出不同的散列值)。

最简单的散列算法就是将输入消息划分成大小固定的块，如 128 位，然后 XOR 每个块，就得到 128 位的散列值。

下面是常用散列算法：

1. SHA（常用）

NIST 开发的 SHA,SHA-1 和 SHA-2 都会考到。SHA 基于 MD4，SHA-1 基于 MD5，

①SHA-1：输入值可以是任意长度（小于 2^{64}=2097152T）；消息摘要长度 160 位；它将消息原文拆分为 512 位的分组的处理，如果长度不够多就填充一些附加的消息。

②SHA-2：SHA-1 已经被发现存在缺陷，SHA-2 就出现了，它有 4 种形式：

*SHA-256，处理 512 比特的分组大小，生成 256 比特的消息摘要。

*SHA-224，处理 512 比特的分组大小，生成 224 比特的消息摘要。

*SHA-512，处理 1024 比特的分组大小，生成 512 比特的消息摘要。

*SHA-384，处理 1024 比特的分组大小，生成 384 比特的消息摘要。

③SHA-3：使用 Keccak 算法，还没发布，至少目前还没有实际破解 SHA-2 的案例。

2. MD2

MD2 是为 8 比特处理器提供的安全散列函数（很老的处理器了）。MD2 处理 16 字节（byte）的分组大小（128 比特），在消息的结尾处添加“校验和”（checksum），生成 128 比特的消息摘要。后来有人证明 MD2 不是单向函数，而且运算很慢，于是它被废止了。

3. MD4

MD4 支持 32 比特的处理器，处理 512 比特的分组大小，通过 3 轮计算，生成 128 比特的消息摘要。不过其最后一个消息分组必须是 448 比特（留 64 比特做什么，书上没写）。

4. MD5

MD5 处理 512 比特的分组大小，通过 4 轮计算，生成 128 比特的消息摘要。与 MD4 一样，它的最后一个消息分组必须是 448 比特（留 64 比特做什么，书上没写）。不管 MD 几，都已经被证明存在散列值冲突了（不同消息得到同一个散列值），专家建议用数字签名来代替。其中，MD5 同一个摘要找出 2 条不同消息的概率约为 264，从一个摘要推算出原文的概率约为 2128。

6.变长散列(HAVAL)

HAVAL 是对 MD5 的更改，处理 1024 比特的分组，运算 3 轮到 5 轮不等，生成 128、160、192、224 和 256 比特的散列值。

不同算法的散列值有多少位是要考的，书上有表格，最好自己归纳。

7.RIPEMD-160

RIPEMD-160 是 RIPEMD-128 的改进版，处理 512 比特的分组，速度是 SHA-1 的两倍，可进行 10 轮共 160 次运算。

8.生日悖论 birthday attack

这个理论是用来破解散列函数的，为了找到散列值的冲突或碰撞。即：

只需要集合 23 个人，其中存在 2 个人生日相同的概率就大于 50%（并不需要 365/2=183 个人）。因为 23 个人两两配对共有 n(n-1)/2=253 个不同的组合，生日共有 365 个不同的日期，出现相同生日的概率是 253/365。相应的，如果集合 100 个人，则两人同生日的概率超过 99.99%。

9.加盐 Salting

为了应对彩虹表的暴力攻击，计算并存储密码的散列值时，要先在原始密码后面加一个随机值，随机值与盐都存在密码文件中。这显著提高了密码被彩虹表破解的难度。

I.9 密码攻击方法（例如暴力破解、唯密文攻击、已知明文攻击）

①分析攻击（Analytic Attack）/代数攻击。分析并利用算法本身的数学逻辑性，找出更简单的替代的算法。

②实现攻击（Implementation Attack）/执行攻击。利用加密程序存在的漏洞，简单易行，破密**首选**。包括 3 种形式：

*旁路攻击 Side-channel analysis，依靠能量消耗、放射性等密码系统运行时的物理属性来攻击，如计时分析和电磁差分分析。

*故障分析 Fault Analysis，通过注入错误信息来对比、记录、分析系统的加密漏洞。

*探测攻击 Probing Attacks，在密码模块周边进行探测和注入，希望能采集到算法或密

钥什么的。

③统计攻击（Statistical Attack）。利用密码系统的统计弱点，例如无法真正生成随机数，浮点运算的错误等。统计攻击试图发现运行密码系统的硬件或操作系统的漏洞。

④穷举攻击（Brute Force/Exhaustive search）。暴力攻击。为了提高速度，通常使用彩虹表。密码一般以散列值的方式存在数据库里，彩虹表是预先计算和整理出的散列值映射表，可以大幅提高猜解速度。

⑤仅知密文/唯密文攻击（Ciphertext Only Attack）。最难的攻击，因为只有几条密文，其它啥也没有。只能通过频率分析进行统计学的攻击和预测。因为 26 个字母中，E,T,O,A,I,是出现频率最高的。

⑥已知明文攻击（Known Plaintext）。手上有明文，也有密文，然后想办法破解。

⑦选定密文/可选密文攻击（Chosen Ciphertext）。手上有密文，只有部分密文有明文。

⑧选定明文/可选明文攻击（Chosen Plaintext）。可以加密部分明文得到密文。

⑨中间相遇攻击（Meet in the Middle）。面向加密运算，通过计算查找出密钥对（K1 加密的密文可以用 K2 解密），便两轮加密算法即双重 DES(2DES)的实际强度和一轮加密一样。

⑩中间人攻击（Man in the Middle）。面向通信链路，在攻击者以通信代理的方式插入收发又方的通信，截获所有数据流。

⑪生日攻击（Birthday）。也称为冲突攻击或逆向散列匹配，利用生日悖论来进行穷举攻击和字典攻击，寻找可以生成相同消息摘要的不同消息。

⑫重放攻击（Replay）。既然破不了密，就截获加密的消息，下次直接重复使用它来进行身份验证什么的。如果系统有时间戳，这个方法就不能用了。

⑬微分/差分密码分析(differential cryptanalysis)。

差分密码分析攻击以找出加密密钥为目标。这种攻击会查看对具有特定差异的明文进行加密而生成的密文对，并且分析这些差异的影响和结果。它在 1990 年作为一种针对 DES 的攻击发明出来，后来演变成为一种针对 DES 和其他分组算法的成功而有效的攻击。攻击者使用两条明文消息，并在它们经过不同的 S 盒时跟踪分组上发生的变化(每条消息都以相同的密钥加密)。得到的密文中已确定的差异用于推测不同可能密钥值的概率。攻击者使用其他几组消息继续上述过程，并检查公共密钥概率值。随着加密过程中的大多数可能值都被用到，密钥也就逐渐显露出来。由于攻击者选择不同的明文消息进行攻击，因此它也是一种选定明文攻击。

⑭线性密码分析(linear cryptanalysys)。是一种已知明文攻击，利用线性近似来描述块密码的行为。如果有足够多的明文和相应密文对，便可得到有关密钥的少许信息，而数据量的增加通常会给成功带来更高可能性。

⑮彩虹表。彩虹表是对散列输出进行过分类处理的查询表，相当于密码字典的作用，提高了破解速度。

⑯因子分解攻击。以 RSA 算法为目标。由于该算法用大质数的乘积生成公钥和私钥，这种攻击试图通过分解这些数的因数来找出密钥。

⑰逆向工程。这种攻击很常用。买一套同款的密码系统，反编译来分析算法找漏洞。

⑱社会工程。坑蒙拐骗、威逼利诱什么的。

J. 应用安全原则于场地与设施设计（遵循安全原则设计场地和设施）

场地的选择很重要，有很多标准很原则，都不难。这有一个新的设计理念：经常被称为环境设计预防犯罪(CPTED)crime prevention through environmental design。指导思想是通过结构化的物理环境和周围环境设计在潜在的罪犯作出任何犯罪行为之前影响其个人决定。

站点选址很简单，不说了。考虑什么可见性、周围区域和外界条件、可达性和自然灾害。

1. 场地规划

场地规划的唯一最重要目标是确保生命、财产和运行安全。

①道路设计

尽管直线可能是效率最高的路程，但设计者应该考虑将道路系统设计成可以将车辆速度降至最低，从而使道路本身成为一种保护屏障。直线或垂线接近设施的道路设计方案不可采用，因为这会使车辆有机会积攒起撞击或冲进建筑物的速度。相反，道路应该与建筑物的周界平行，再配以天然土台、高路牙、树木或其他屏障，用以防止车辆驶离道路。

②窗户

应该通过镶装玻璃、加框、建筑物正面支撑墙铆钉固定等涉及窗户的操作来抑制发生爆炸事件时玻璃飞溅造成的危害。为了保护建筑物内人员，要充分考虑玻璃的特性，做好玻璃与窗框的衔接、窗框与建筑结构的固定，形成一个平衡的整体。

*窗户不应安在门旁，因为窗户打开时可以让人摸到门并打开门锁。

*用夹层玻璃取代普通玻璃，给窗户安上防护栏，以防被人翻窗而入。

*落地窗应该无法打开，应该用栏杆和报警器保护起来。

*窗用报警器应该配有磁开关，当磁体被分开时(例如窗户打开时)，报警器报警：四层楼以下的窗户都应安装这种保护装置。

*考虑使用可以安全固定或水泥浇筑在四周建筑结构中的钢制窗框。

③玻璃的类型

*钢化玻璃，类以于汽车的挡风玻璃。具有抗碎性，即便被撞，也只会碎成小块晶体，不会形成尖锐的玻璃碴。钢化玻璃可用在入口门和邻近的面墙上。

*夹丝玻璃，可抵抗钝器的击打。玻璃中镶有金属丝网，因此可以提供有限的保护。

*夹层玻璃，建议临街窗户、门廊和其他访问区安装夹层玻璃。夹层玻璃由两篇普通玻璃组成，中间隔着一个弹性塑料片。玻璃受撞击时虽然会碎，但碎玻璃会粘在内层塑料材料上。

*防弹(BR)玻璃，通常安在银行和高风险区域。防弹玻璃有多种不同的玻璃层，标配为 1.25 英寸厚，可抵御 9 毫米子弹的冲击。

④玻璃破碎传感器

玻璃破碎传感器对于装有大量玻璃门窗的建筑物是一种非常好的入侵检测设备。玻璃破碎传感器的基本类型包括：

*声学传感器。监听与玻璃破碎频率相匹配的声学声波。

*振动传感器，探测玻璃破碎时的振动波。

采用双重技术的玻璃破碎传感器——即同时监测声波和振动波——效果最佳。

⑤车库

*使用引导标示，给车辆和行人指引设施出入口。

*用闭路电视系统监视事件，在车库安装紧急呼叫盒。

*安装明亮灯光是预防事故和攻击的最有效手段之一。

*建议车位照明度为 10-12 英尺烛光，人行和驾驶通道为 LS-20 英尺烛光。

*停车设施外部安装高亮度照明，尤其是行人交通密集的区域。

*制定规定外部照明应离地面约 12 英尺，应该可向下照射广阔的地面。

*把建筑物外墙刷成可反射灯光的白色，以增加能见度。

*战略性布局照明灯具，使灯光可以从墙壁反射，以减少可供犯罪分子或攻击者藏身的黑暗角落。

*如果车库在设施底层，电梯或楼梯应只通控制区外面的大堂。

*所有员工和来访者均应受控接待区经过，以保持没施的完整性；通过这种方式，可进入建筑物核心地带的电梯将只能从大堂而不是车库层进入。

2.地点威胁

①自然威胁的类型

美国联邦应急管理局(FEMA)认为自然威胁包括以下几项：

飓风、龙卷风、地震、森林火灾、泥石流、洪水。

②灭火系统

火需要三个元素齐备才会燃烧：热、氧和燃料源。灭火器和灭火系统通过消除其中一个元素来灭火。水是主要灭火工具，但也会给电子设备带来极大伤害，根据火灾类型的不同，灭火器共分四类（普水电金）：

***A 类灭火器**应对**普通**易燃材料火灾，如纸、木头、纸板和大多数塑料。这类灭火器的数字级别表明它的含水量和可以扑灭的火量。

***B 类灭火器**应对可燃或易激**液体**火灾，例如汽油、柴油、油脂和石油。这类灭火器的数字级别表明它可以扑灭多大面积的火。

***C 类灭火器**应对的火灾涉及**电气**设备，如家电设备、线路、断电器、电源插座。决不可用水来灭 C 类火灾——触电的风险太大!C 类灭火器没有数字级别。C 类意味着灭火剂不导电。

***D 类灭火器**最常出现在化学实验室，用于应对易燃**金属**火灾，例如镁、钛和钠。这类灭火器既没有数字级别，也没有多用途级别。它们的设计只针对 D 级火灾。

3.公用设备方面的考虑

①供电

*应急和常规配电板，导管和开关装置分开安装在不同位置，尽可能远离。电力分配也应在不同的地点运行。

*应急电机应安装在远离装货码头、入口和停车场的地方。比较安全的地点包括楼顶、受保护地坪和受保护内部区域。

*电机的主要燃料储罐应安置在远离装货码头、入口和停车场的地方。对这些储料罐的访问应受严格限制和保护，其中包括罐盖上锁和密封。

②通信

通信设备也是企业核心公用设备的一大组成部分。应考虑配备备用电话服务来保持发生事故时的通信通畅。对于大多数机构来说，应该给特定员工配备移动电话，或者机构保留一份电

话联系单，上面列出所有关键员工和他们的移动电话号码。

③公用设备

为了把发生灾害后出现关键故障的可能性降至最低，应采取以下措施：

*如果可能，把公用设备安置在地下遮蔽起来并提供严密保护。

*如果没有冗余电源可用，考虑快速连接便携公用设备备用系统。

*确保检修孔等访问点的安全，保护饮用水源免受水传播污染物污染。如果必要，对水进行常规测试，帮助检测水传播污染物。

*把标识关键公用设备的标志尽可能做小。用护栏防止未经授权访问，利用绿化景观掩蔽地面上的系统。

*把汽油、石油和润滑油储罐及其操作间安置在地势低于所有其他建筑物的地点。燃料储罐应远离建筑物至少 100 英尺。

*公用设备系统至少远离装货码头、前门入口和停车场 50 英尺。

K. 设计和实施物理安全

第三域的物理安全都是宏观的、外部的；第七域的物理安全都是具体的、内部的。

联邦应急管理局(FEMA)以“风险管理系列”（RMS）的形式发布广泛指南，致力于从设计上指导如何抑制多重危险事件。该系列包含一大批有关人为灾害的出版物，旨在提高建筑物的安全性，降低预计的恐怖袭击对建筑物的潜在影响。该系列的目的是减少建筑物及其相关基础设施的结构和非结构构件受到的物理损害，减少常规炸弹，化学、生物和放射制剂，地震，洪水和狂风造成的人员伤亡。该系列的预期对象包括为私人机构工作的架构师和工程师、建筑物业主/经营者/管理者、负责建筑学领域工作的州和地方政府官员。

为具体环境设计物理安全性时，需要牢记控制措施的功能顺序：

1. **阻拦/威慑** Deterrence 安控措施应当打消坏人对非法访问的念头(边界限制)。
2. **拒绝** Denial 阻拦失败，应当拒绝对物理资产的直接访问(关闭保险库大门)。
3. **检测** Detection 拒绝失败，系统就需要检测入侵(使用运动探测器)
4. **延缓** Delay 最后要充分地延缓入侵，以便快速响应并处置。(设备上锁)

一个组织机构的物理安全计划应当涉及下列**目标**：

①通过震慑预防犯罪和破坏——栅栏、保安、警示标志等。

②通过使用延迟机制来减少损失——延缓对手行动的防御层，如锁、安全人员和屏障。

③犯罪或破坏检测——烟雾探测器、运动探测器、CCTV 等。

④事故评估——保安检测到的事故的反应以及破坏级别的确定。

⑤响应措施——灭火机制、应急响应过程、执法通告、外部安全专家咨询。

K.1 配线间

1.接线柜的安全策略有：

*从不把配线室作为一个通用的存储区。

*有足够的锁。

*保持区域的整洁。

*不要存放易燃易爆物品的区域。

*设置视频监控监控内部的配线间站动。

*使用门打开传感器日志条目。

*不要把钥匙给除了授权管理人员之外的任何人。

*对配线间的安全和内容定期进行检查。

*把配钱间纳入组织的环境管理和监控，以确保有适当的环境控制和监测，以及检测破坏性条件，如洪水或火灾。

2.电缆设施管理

电缆设施的关键成分包括入口设备、设备机房、主干电缆、主干线架设通路、通信机房和水平配线系统。

3.防雷电保护

雷电击中某个接地系统会造成地电位或接地电位上升(GPR)。与这个接地系统连接的有线通信的任何设备都极可能被这股寻求远程接地的输出电流毁坏，损伤有时不会马上显现，这就是所谓的潜在损伤，导致设备出现过短的“平均故障间隔时间”（MTBF)。

最好的防雷就是用光缆，但这成本太高了。设备防雷工程可以是将有线通信与远程地面隔离，通过使用光学隔离器或隔离变压器实现。这套装置组合在一起，安装在绝缘的机柜表面，称作高压接口(HVI)。HVI 在接地电位上升(GPR)期间隔离设备，阻止任何电流从高电势接地系统流向低电势接地系统，可完全保护任何设备或在设备上工作的的人员免受损害或伤害。

K.2 服务器机房

服务器机房需要比设施其他地方级别更高的安全保护。其中包括一个受严格保护的无窗户和只有一个受管控入口的房间。切记，服务器一旦被人入侵，整个网络都将暴露在风险之下。

1.机架安全

机架锁可确保只有正确的人才可以访问服务器，只有负责通信的人才可以访问通信设备。“可管理”机架锁可在远程配置，仅限于特定人员在特定时间需要时访问，可减少事故、破坏或未经授权安装恰设备(有可能毁坏性增加耗能和机架温度)的发现。

2.受限工作区安全

像政府敏感信息隔间设施(SCIF)这样的受严格限制的工作区一样，需要增加安全措施，以确保对这些区域的访问受到更严格的限制。

此外，服务器房间应设在建筑物的核心。尽量避免在放置在底层、顶层和地下室。服务器房间应远离水、气和污水管道，这些管道泄漏或泛滥的风险太大，可能会造成严重的损坏和故障停机时间。服务器机房的墙壁还应当至少达到 1 小时防火时间的防火等级，而存放纸质和存储介质的房间墙壁要至少防 2 个小时的火。

K.3 介质存储设施

没什么内容，都很浅显。

K.4 证据存储

保留日志、审计和其他数字事件的记录是十分重要的，可用于内部企业调查或和执法为基

础的电子取证。

K.5 限制区和工作区安全 （例如：运营中心）

进入含有更高价值或重要性资产的区域应该受到限制。例如，只有网络管理员和安全人员才能够进入服务器机房。核心区域必须从地板到天花板之间全部封闭。要防止肩窥（在身后窥视操作者的显示器或键盘动作来收集信息）。

K.6 数据中心安全

有数据中心的单位，这个数据中心一定是核心要素了，其安全至关重要。

1.智能卡 Smartcards

智能卡形式多样，包含了经过授权的可以被用于身份识别和或身份验证目的的持卡人信息。有的智能卡具有处理信息的能力或存储了一定数量的数据。如果智能卡丢失了，很可能被冒用，于是最常用的多因子认证方式还要求使用 PIN 码。

还有什么无记忆的卡、接近式读卡机（Proximity Readers）都很好理解，不多说。

2.入侵检测系统 Intrusion Detection Systems

这里讲的是物理的入侵检测，包括保安人员、自动化访问控制措施、运动探测仪以及其他特殊的监控技术。一般都是通过检测电流的变化或者通信的通断来预警意外情况。

3.电磁放射的保护 Emanation Security

用于阻止放射攻击的对策和防护手段被称为瞬时电磁脉冲设备屏蔽技术(TEMPEST)设备。TEMPEST 最初是一个政府研究项目，现在防止放射截获的一系列方法的统称。主要有 3 种：

①法拉第笼/屏蔽网/Faraday Cage

只要有金属屏蔽网，电磁信号就传不了。

②白噪声 White Noise

白喋声指的是一直广播虚假通信数据，从而掩盖和隐藏实际存在的放射信号。

③控制区 Control Zone

控制区只是在受保护区域环境内实现法拉第笼或白噪声，在受保护区域环境外则不采取任何措施。受控区一般是涉密单位都有的“屏蔽机房”，也可以是一层楼或整座建筑。

4.人员出入控制

①内部捕人陷阱。

②双门入口。双门入口一次只允许一个人进出，只有等内门关闭后外门才会打开。双门入口可增设生物测量装置，必须在内门打开之前激活。

③“两人”规则。即在一个区域内必须有两个人结伴在一起，不可一人独自逗留。

K.7 公用设施和供热通风与空调系统考虑事项

1.公用设施和电力

数据中心要有双路电源引接，并且有 UPS 和发电机组。

2.不间断电源(UPS)

UPS 只能维持供电一小段时间，但往往足以应对电力公司的小故障或短时停电，也可以让设备有机会正常关机。时间长了就要发电。UPS 另一个重要功能是可以稳压和电涌保护。

3.发电机

发电机应该最快在发生停电故障后的 10 秒内启动。

4.电涌保护

电涌保护器包含一个保险丝，它在电源功率剧烈变化而造成对设备的损坏之前熔断。因为它会造成突然断电，对设备还是有伤害的，不如使用 UPS。什么是电涌？下面这些都是要考的电源专业词汇：

*故障(fault) 电力的瞬间/短时消失。——*断电/中断(blackout) 电力完全/长时消失。

*衰变/电压不足(sag) 瞬间电压降低。——*降压/电压过低(brownout) 长时间低电压。

*脉冲/尖峰(spike) 瞬间高电压。——*电涌/浪涌(surge) 长时间的高电压。

*瞬时现象(transient) 短时间的线路干扰。——*噪声(noise) 持续不断的电源干扰。

*平稳(clean) 完全平稳的电流。

*接地(ground) 电路中的电线是接地的。

*起动功率(inrush) 脉冲和电涌通常在连接电源时发生（插拔）。瞬时涌流/励磁涌流

5.噪声 Noise/电磁干扰

由电流产生的噪声会影响任何一种依赖于电磁传输机制的数据传输，例如电话、蜂窝电话、电视、音频、无线电和网络机制。手机靠近电脑、电视什么接电话，肯定有嗞嗞嗞的声音。

电磁干扰(EMI) electromagnetic interference 有两种类型：

普通模式 Common mode 噪声是由电子设备的火线和地线之间的电势差产生的。

导线模式 Traverse mode 噪声是由电子设备的火线和零线之间的电势差产生的。

射频干扰(RFI) Radio frequency interference 与 EMI 一样，影响许多系统。RFI 由很多常见的电器所产生，包括荧光灯、电缆、电子加热器、计算机、电梯、电动机和电磁铁等。

6.散热、通风和空调(HVAC)

机房保持温度在华氏 60 到 75 度之间(摄氏 15 到 23 度)，湿度应当维持在 40%和 60 %之间。湿度太高会导致侵蚀，湿度太低则会导致产生静电。

缩略语 HVAC 代指散热、通风和空调。热会使处理器速度减慢并停止执行程序，从而给计算机设备带来广泛损害，甚至会使焊接变松乃至完全断开。过热会降低网络性能和造成宕机。数据中心和服务器机房需要配备不间断散热系统。

K.8 供水问题 （例如：渗漏、洪灾）

水会搞坏设备的。有些地方的水不容易被发现和重视：

*通风系统发生堵塞后，潮湿的热空气将无法快速流动，从而造成冷凝；

*如果通风口位于机器上面或后面，会看不到冷凝形成的小水珠；

*若不能适当清除冷凝，单机空调特别容易形成漏水；

*进风口附近哪怕只聚积少量水，也会提升湿度，使服务器充满潮气。

K.9 火灾预防、探测和灭火

火灾方面肯定会出考题的。

1.燃烧的三要素：燃料 fire,、高温 heat 和氧气 oxygen。

各种灭火方法是通过阻断燃烧的哪个要素来实现的，这不难。

2.起火的四个阶段：

①阶段 1：开始阶段，空气电离，不存在冒烟。

②阶段 2：冒烟阶段，起火点出现烟雾。

③阶段 3：火焰阶段，肉眼能够看到火焰。

④阶段 4：高温阶段，起火时间已经相当长，此时温度极高，并所有东西都在燃烧。

数据中心发生的大多数火灾都是由配电插座过载导致的。

3.灭火器 Fire Extinguishers/火灾类型/普液电金

A	普通的易燃品 Common combustibles	水、苏打酸，干粉、专用液体 Water, soda acid (a dry powder or liquid chemical)
B	液体，Liquids	二氧化碳、哈龙、苏打酸/CO2,halon,soda acid
C	电气，Electrical	二氧化碳、哈龙/CO2,halon
D	金属，Metal	干粉/Dry powder

4.防火检测系统 Fire Detection Systems

①火焰激发系统。根据火焰的红外线能量来触发灭火抑制装置。

②烟感系统。根据光电或放射性电离传感器来触发灭火抑制装置。

③温感系统。包括固定温度（高于 XX 度）或升温速度（每分钟升 15 度）探测器。

5.放水灭火系统 Water Suppression Systems

目前有四种主要的放水灭火系统。

①湿管道系统 wet pipe system (也称为封闭头系统 closed head system)。管里一直有水，当灭火装置被触发的时候，就会立刻放水。

②干管道系统 dry pipe system。管中是压缩空气，当灭火装置被触发的时候，先排队空气，再放水。

③洪水系统/密集洒水 deluge system。是干管道系统的另外一种形式，它使用较粗的管道，因此能排出大股的水流。这显然不能用在机房。

④预先响应系统/预作用 preaction system。是干/湿管混合系统。平时都是干管，有烟、热等火灾症候时（温度上升），预先充水，但不打开喷水阀门；如果喷水头受到临界高温了，就自动喷水；如果还没到触发的高温，火灾已经被灭或者没有发生，就手动把水再抽回去。

6.气体释放系统 Gas Discharge Systems

气体释放系统通常比放水系统更有效，机房经常用到。不过，气体释放系统会排除氧气，对人是非常危险的。使用的气体有主要：

①二氧化碳 CO2

②哈龙 halon（二氟二氯甲烷）：好用，但在华氏 900 度的时有毒且破坏臭氧层（氯氟烃）。

③FM-200(哈龙最好的替代物)，是一种无色液化压缩气体，不会影响视线，不置换氧气，可用于有人的空间。还有别的替代物：NAF-S-ID、CEA-410、CEA-308、FE-13、烟烙尽(Inergen)、氩气(Argon)、氮氩气(Argonite)什么的。

7.火的破坏性

①烟会损坏存储设备；热会损坏所有电子设备。

②华氏100度会损坏存储磁带；175度损坏CPU内存等设备；350度损坏纸质材料。
③灭火介质（水、干粉、化学品）会引起短路，腐蚀设备。
④消防员强拆会破坏设施。

第四域　通信与网络安全 （设计及保护网络安全）

Chapters 11,12 in OSG 7th

Chapters 6 in AIO 6th

A.应用安全设计原则于网络架构（例如：IP 协议与非 IP 协议，网络分段）

本域由 4 大内容组成（偏重技术，无管理）：

A.什么是网络（结构、协议）；B.网络怎么连（方法、组件）；

C.信息怎么传（格式、通信）；D.安全怎么做（措施、攻击）。

A.1 OSI 与 TCP/IP 模型

一、分层模型

网络通信一般是按层描述。几种不同的分层模型存在；最常用的是：

*参考模型，分为七层(物理层，数据链路层，网络层，传输层，会话层，表示层，应用层)

*TCP/IP 或(DoD)模型，分为四层（链路层，网络层，传输层，应用层），是个协议栈。

怎么理解和记忆两种模型、上下的封装关系，搞网络的一般都清楚。

通信类型	OSI 模型	TCP/IP 模型	运用场景	
数据流(应用消息)-Date(Message)	Application	Application	主机	
数据类型-Format	Presentation			
应用连接-会话-Session	Session			
段 Segment(TCP) 报文 Dategram(UDP)	Transport	Host-to-host	逻辑连接	
包-Packet	Network	Internet	IP 网	
帧-Frame。细分 2 层： 逻辑链路控制 LLC+介质访问控制 MAC	Data link	Network access	通信网	以太网
比特/位-Bits	Physical			承载网

TCP/IP 既是分层协议（分四层），也是聚合协议（聚合了七层里的部分层，也融合了很多协议共同工作）。

二、各层协议

第一层：物理层

这一层定义了网络的物理拓扑。这一层是只关心物理信令。只有硬件处理信号在这层定义：这些都是：电缆，连接器，集线器和中继器等。

- EIA/TIA-232 and EIA/TIA-449
- X.21
- High-Speed Serial Interface (HSSI) 高速串行接口
- Synchronous Optical Network (SONET) 同步光网络
- V.24 and V.35

第二层：数据链路层

数据链路层接收来至于网络层的数据包(Packet)，生成在网络中传输的数据帧(Frame)。

这一层确保与通信对端信息交换的无误(或容错)。如果数据链路层检测到帧里面的错误，它将请求对端重新发送该帧。数据链路层将信息从更高层进行格式转化，该转化基于某种网络技术，如以太网，令牌环网等等。这一层使用硬件地址发送帧到对端设备，只是做物理的连接。数据链路层关注的是将数据帧发送到下一跳链路。二层网络通信技术有以太网 Ethernet(IEEE 802.3),令牌环网 Token Ring (IEEE 802.5),异步传输模式 ATM(asynchronous transfer mode),光纤分布式数据接口 FDDI(Fiber Distributed Data Interface),和铜线分布式数据接口 CDDI(Copper DDI)。

该层其实还细分了两层，上面的 LLC 子层(IEEE 802.2)和下面的 MAC 子层(IEEE 802.3)。

第二层必须要讲讲 MAC 地址：

该层要向数据帧添加硬件的源地址和目的地址，硬件地址指的是介质访问控制(MAC)地址(Media Access Control address)，它是一种用十六进制表示法表示的 6 字节(48 比特)二进制地址，例如 00-13-02-1F-58-F5。前三个字节(24 比特)代表物理网络接口（网卡）的供应商或制造商，这被称为组织唯一标识符(OUI) Organizationally Unique Identifier；后三个字节(24 位)是设备的唯一代码。世界上没有两个设备具有相同的 MAC 地址（中国的山寨网卡就有可能一样）。

讲了 MAC 地址就要知道 MAC-48、EUI-48 和 EUI-64（考点）：

MAC-48 和 EUI-48 一样，都是 6×8=64 位，前者用于网络设备，后者用于其它设备和软件。而 EUI-64 是为了适应 IPv6 协议和激增的网络设备，而出现的新的地址标准，它向下兼容，具体表示方法就是：

MAC-48 在中间加 FF：FF，比如：cc：cc：cc：FF：FF：cc：cc：cc

EUI-48 在中间加 FF：FE，比如：cc：cc：cc：FF：FE：cc：cc：cc

链路层支持的协议有：

- Serial Line Internet Protocol (SLIP) 串行线路网络协议
- Point-to-Point Protocol (PPP) 对点协议
- Address Resolution Protocol (ARP) 地址解析协议：将 IP 地址解析为 MAC 地址
- Reverse Address Resolution Protocol (RARP) 反向地址解析协议：MAC 解析为 IP
- Layer 2 Forwarding (L2F) 二层转发协议
- Layer 2 Tunneling Protocol (L2TP) 二层隧道协议
- Point-to-Point Tunneling Protocol (PPTP) 点对点隧道协议
- Integrated Services Digital Network (ISDN) 综合服务数字网络

第三层：网络层

数据链路层使用硬件寻址(MAC)，网络层则使用逻辑地址寻址(IP 寻址体系)。网络层向数据中添加路由信息和寻址信息（源和目的 IP 地址），负责路由选择和传送信息，也管错误检测和节点数据通信(也就是通信控制)，但不对传输进行验证(由传输层负责验证)。

网络层的典型协议有：

- Internet Control Message Protocol (ICMP) 网络控制报文协议
- Routing Information Protocol (RIP) 路由信息协议
- Open Shortest Path First (OSPF) 开放式最短路径优先

■ Border Gateway Protocol (BGP) 边界网关协议

■ Internet Group Management Protocol (IGMP) 网络组管理协议（用来多播）

■ Internet Protocol (IP) 网络协议

■ Internet Protocol Security (IPSec) 网际协议安全

■ Internetwork Packet Exchange (IPX) 互联网分组交换协议

■ Network Address Translation (NAT) 网络地址转换

■ Simple Key Management for Internet Protocols (SKIP) 网络简单密钥管理协议

■ Dynamic Host Configuration Protocol（DHCP）动态主机配置协议（IP 分配）

最重要的是 **IP 协议**，有两大功能：

①寻址：IP 协议使用 IP 目的地址通过网络进行转发数据包，直至该数据包到达目的地。

②分段：如果数据包大小大于本地网络允许的最大数据值，IP 协议将该数据包拆分。

IP 是无连接的协议，不保证传输的可靠性。

最广泛的还有路由协议，考试涉及的动态路由协议有：

①距离矢量 distance vector。距离矢量路由协议维护一个目的网络以及距离和方向的跳数的列表(也就是到达目的地所经过的路由器数量) 有 RIP、IGRP、EIGRP。

②链路状态 link-state。链路状态路由协议维护一个所有已连接网络的拓扑图，并且使用这个拓扑图确定到达目的地的最短路径，有 OSPF 和 IS-IS。

BGP 是外部路由协议(EGP)，不适用于上述两种分类，有题目认为是路径矢量 path-vector。

过去常用的**非 IP 协议**有：

IPX、AppleTalk 和 NETBUI。（虽然过时了，但这些协议是可以绕过防火墙的）

①互联网分组交换协议 IPX 是 IPX/SPX 协议套件常用的，使用于上世纪 90 年代的 Novell NetWare 网络。

②AppleTalk 协议是一套由苹果公司开发并使用于 Macintosh 系统网络上，最早版本于 1984 初发布。2009 的 Mac OS v10.6 版本发布后取消了苹果操作系统对 AppleTalk 的支持。IPX 和 AppleTalk 都可以通过 IP 协议网关实现死区网络与 IP 网络的互联（死区是使用非 IP 协议网络的网段）。

③NetBIOS Extended User Interface/NetBIOS 扩展用户界面（NetBEUI 又名 NetBIOS 帧协议或 NBF），是微软最广泛认知的一个协议，于 1985 年开发并用于支持文件和打印机共享。微软通过使用 NetBIOS over TCP/IP (NBT)技术，使 NetBIOS 工作于 TCP/ IP 协议上，从而仍能运用于现代网络。NetBIOS 端口（**127-139**）已成为流行的网络蠕虫攻击的目标，基于 NetBIOS 实现的弱点被循环利用，但问题不在协议自身。但作为一个低层协议，NetBIOS 已不再获得支持，只有它的 SMB（Server Message Block）和 CIFS（Common Internet File System）的变种仍在使用。

其它需要了解的协议：

ICMP 网络控制报文协议

就是 ping 、traceroute 、pathping。ICMP 最重要的应用就是拒绝服务攻击了。第九域有归纳，这里简介一下：死亡之 ping 发送一个畸形的大于 65535 字节数据包给一台计算机并试图让其崩溃。Smurf 攻击通过欺骗广播 ping 对目标网络产生巨大的流量。ping 数据包泛洪

是一个基础的拒绝服务(DoS)攻击，它消耗目标可用的所有带宽。

DHCP 分配出租 IP 地址的 4 步流程：The four-step DHCP lease process is：

1.发现 DHCP。DHCP DISCOVER message

2.响应发现。DHCP OFFER message

3.请求地址。DHCP REQUEST message

4.响应请求。DHCP ACK message

第四层：传输层

传输层负责管理连接的完整性并控制会话。传输层接收来自于会话层的 PDU（Protocol Data Unit），比如：协议数据单元、数据包单元、数据负荷单元等，并将其转换为数据段。会话规则指定每个数据段中可以包含多少数据、如何验证传输数据的完整性、如何确定数据是否丢失。会话就是端到端的一个逻辑通信连接。该层协议有：

- Transmission Control Protocol (TCP) 传输控制协议
- User Datagram Protocol (UDP) 用户数据报协议
- Sequenced Packet Exchange (SPX) 顺序数据包交换
- Secure Sockets Layer (SSL) 安全套接字层
- Transport Layer Security (TLS) 传输层安全

用户数据报协议(UDP)和传输控制协议(TCP)是最重要的传输层协议，详见 TCP/IP 模型。

第五层：会话层

会话层负责在两台计算机之间建立、维护和终止通信会话（使用会话）。这一层管理对话模式或对话控制(单工、半双工、全双工)，并为分组和恢复建立检查点，以及重新传输上一次验证检查点以来失败或丢失的 PDUs。该层协议有：

- Network File System (NFS) 网络文件系统
- Structured Query Language (SQL) 结构化查询语言
- Remote Procedure Call (RPC) 远程过程调用
- Network Basic Input Output System（NetBIOS）
- PAP 密码认证协议 Password Authentication Protocol
- PPTP 点对点隧道协议 Point-to-Point Tunneling Protocol
- DNA SCP Digital Network Architecture Session Control Protocol.

第六层：表示层

表示层负责将从应用层接收的数据转换为遵从 OSI 模型的任何系统都能理解的格式，如：将 Unicode 编码的数据转换为 ASCII 或 EBCDICM 字符集。它向数据中强行添加通用的或标准的结构和格式化规则。表示层还负责加密和压缩。因此，它成为网络和应用程序之间的接口。通过确保数据格式能够被两个系统支持，表示层准许不同的应用程序通过网络交互。大多数文件或数据格式在这一层上出现，包括图像、视频、音频、文档、电子邮件、Web 页面和控制会话等格式。该层协议有：

- American Standard Code for Information Interchange (ASCII) 美国信息交换标准代码
- Extended Binary-Coded Decimal Interchange Mode (EBCDICM) 扩充二进制编码的十

进制交换码

■ Tagged Image File Format (TIFF) 标签图像文件格式

■ Joint Photographic Experts Group (JPEG) 联合图像专家组

■ Moving Picture Experts Group (MPEG) 运动图像专家组

■ Musical Instrument Digital Interface (MIDI) 音乐设备数字接口

第七层：应用层

本层为应用或者操作系统，提供网络接收或者发送服务，负责将协议栈与用户的应用程序、网络服务或操作系统连接在一起。应用程序并不位于应用层内，只是通过相关的协议来对外通信。该层协议有：

■ Hypertext Transfer Protocol (HTTP) 超文本传输协议

■ File Transfer Protocol (FTP) 文件传输协议

■ Line Print Daemon (LPD) 行式打印机后台程序

■ Simple Mail Transfer Protocol (SMTP) 简单邮件传输协议

■ Telnet 远程登录

■ Trivial File Transfer Protocol (TFTP) 普通文件传输协议/主要用来更新设备的配置文件

■ Electronic Data Interchange (EDI) 电子数据交换

■ Post Office Protocol version 3 (POP3) 邮局协议第三版

■ Internet Message Access Protocol (IMAP) 互联网消息访问协议

■ Simple Network Management Protocol (SNMP) 简单网络管理协议

■ Network News Transport Protocol (NNTP) 网络新闻传输协议

■ Secure Remote Procedure Call (S-RPC) 安全远程过程调用

■ Secure Electronic T ransaction (SET) 安全电子交易

三、TCP/IP 模型

TCP/IP 模型也称为 DARPA 或 DOD 模型，和 OSI 的对比前面已经讲了，分四层：

④应用层 Application，没什么好讲的

③传输层 Transport（也称为主机到主机层 Host-to-Host），包括 TCP 和 UDP 协议。

②网络层 Internet（也称为互联网层 Internetworking），包括 IP、ICMP、IGMP 等协议。

①网络接入层 Link（网络接口层 Network Interface/网络访问层 Network Access）。

重点讲下 TCP/IP 在传输层的传输控制协议 TCP 和用户报文协议 UDP 协议。

①UDP 是一种无连接的、不可靠的协议。这并不意味着 UDP 设计不佳。相反，应用层将执行错误检查，而不是该协议。UDP 常用于传输音频和视频。它的报头很简单，四个字段：

1.源端口 Source port；2.目的端口 Destination port；3.报文长度 Message length；4.校验和 Checksum。

②TCP 是面向连接、可靠的协议，提供无差错传输保证完整性。

***TCP 三次握手**确保通信会话的建立的可靠性，其描述如下：

1.客户端（源）向服务器发送 SYN (同步)数据包。

2.服务器（目的）使用 SYN/ACK (同步和确认)数据包响应客户端。

3.客户端使用 ACK(确认)数据包响应服务器。

*如果要**结束会话**，有两种方法断开：

1.最常用的方法是使用 FIN (finish) 数据包来代替 SYN 数据包；收发双方都要发一个 FIN 包，对方通过 ACK 确认，完成中断要产生 4 个包。

2.使用 RST (reset) 数据包够使会话立即和突然终止。

*TCP 的数据包完整性和顺序的确认：

通过 TCP 报头中的序列值（sequence number）来确认收到数据包的顺序。接收方不一定每收一个包都要回复一个确认信息，如果信道质量好，可能一次多了好多包以后再回复确认；回复确认之前传输的数据包数称为**传输窗口**（transmission window），只有一个窗口里的数据都确认了，再发下一组的数据。这就是所谓的滑动窗口机制，窗口越大速度越快，但如果丢包率高，那速度就大打折扣了。当然，这个窗口值是可以动态变化的。

下面介绍 **TCP 报头**。前面讲了很多“包”，其实传输层应该叫段（TCP）和报文（UDP），这里混用了。与 UDP 协议相比，TCP 报头相对复杂，长度为 **20 到 60** 字节，有这么些内容要了解（数字是占多少比特位），还有些字段是不会考的，没列出来。报头字段分配：

源端口-16，目的端口-16；序列号-32，窗口大小-16；预留-4，可变量-（32 的位数）；标志-8（flag）。

这个“标志”flag 指示了 TCP 数据包的功能，并且请求接收方采用特定的方式进行响应。标志字段的长度为八个比特，代表了 8 个标志符，其中某个比特位数值为 1 时，它代表的标志符就生效，为 0 则不生效。所以最多可以同时 8 个标志都生效，当然这种情况没有。

1.CWR：拥塞窗口减少 Congestion Window Reduced

2.ECE：拥塞回复 ECN-Echo (Explicit Congestion Notification)

3.URG：紧急数据 Indicates urgent data

4.ACK：确认 Acknowledgement

5.PSH：立即推送数据 Indicates need to push dataimmediately to application

6.RST：重置 Reset，立即中断 TCP 会话 Causes immediate disconnect of TCP session

7.SYN：同步，Synchronization，要求与序列号同步

8.FIN：结束，协商正常结束会话，Finish Requests graceful shutdown ofTCP session

当 TCP 字段封装成 IP 包时，包头会加上协议字段。IP 包里用数值 **6** 来代表这个包里的数据是 TCP 协议发来的。相应的，**1** 表示 ICMP 协议；**2** 表示 IGMP；**6** 表示 TCP；用数值 **17** 表示数据是 UDP 协议；**51** 表示 AH（IPSec 的认证头部）。

③当一个通信连接在两个系统之间建立起来时，它通过端口（port）的使用完成操作。TCP 和 UDP 都有 65536（2^{16}）个端口（16 位）。端口，也被称为套接字（socket）就是通信链接两端传输数据同意使用的地址号。

***保留端口/知名端口/服务端口** well-known ports or the serviceports：**0~1023**。如：

FTP/TCP**20、21**，SSH **22**，Telnet/TCP**23**，SMTP/TCP**25**，DNS/UDP**53**，
终端访问控制器访问控制系统(TACACS+)/TCP**49**，
终端访问控制器访问控制系统 TACACS 和 XTACACS/UDP**49**，
引导协议(BootP)和 DHCP/UDP**67、68**，

普通文件传输协议 TFTP/UDP**69**，
HTTP/TCP**80**，POP3/TCP**110**，网络时间协议 NTP/**12**3，
NetBIOS 服务/**137-139**，
互联网邮件身份验证协议 IMAP/TCP**143**，
SNMP/UDP**161**（162 用于跟踪信息），轻量级目录访问协议 LDAP/TCP**389**、SSL**636**，
HTTPS+SSL 或 TLS/TCP**443**，活动目录 AD/**445**，日志服务/UDP**514**
打印后台程序 LPR、LPD/TCP**515**、**9100**，
下面是已注册端口：
Microsoft SQL Server **1433**，Oracle **1521**，H.323 **1720**，PPTP **1723**
网络文件系统 NFS/TCP**2049**，RDP **3389**，
Diameter 访问控制协议/TCP**3868**，
X 视窗(XWindow)/TCP**6000-6063**，

***注册端口**/已注册软件端口 registered software ports：**1024~49151**。这些端口具有注册到 IANA(www.iana.org)的一个或多个互联软件产品，目的是为客户端连接提供一个标准的端口编号系统。

***动态端口**/私用端口/随机端口 random ports：**49152~65535**。这些端口是随机的、动态的、私用的、临时的使用，没有规定标准的用途。

4.重点看看 IP 协议

IP 是无连接的、不可靠的数据报服务，不保以正确顺序传送数据包，因此，你必须在 IP 上使用 TCP，从而获取可靠的和受控的通信会话。

①IPv4 与 IPv6

IPv4 使用 32 比特的地址，而 IPv6 则使用 128 比特地址。IPv6 提供了作用域地址、自动配置和 QoS 优先值等新功能。作用域地址使管理员能够进行分组以及随后阻止或允许对网络服务(例如文件服务器或打印)的访问。自动配置排除了对 DHCP 和 NAT 的需求。QoS 优先值允许基于优先顺序内容来管理通信。

IP 地址等级与分类已经不知道说了多少遍了：

A 类： 0， 1－126， 255.0.0.0/8；1 个 A 共 16777214 个主机
B 类： 10， 128－191, 255.255.0.0/16；1 个 B 共 65534 个主机
C 类： 110， 192－223, 255.255.255.0/24；1 个 C 共 254 个主机
D 类： 1110， 224－239, D 用于多播；
E 类： 1111， 240－255, E 预留待用；
127：留给环路地址，用于自检排障，尽管实际中只使用了一个 127.0.0.1。
私网/专有地址（RFC1918 定义），A、B、C 各一段，在讲 NAT 的时候会用到：
10.0.0.0/8， 即：10.0.0.0~10.255.255.255，1 整个 A
172.16.0.0/12， 即：172.16.0.0~172.31.255.255，16 个 B
192.168.0.0/16，即：192.168.0.0~192.168.255.255，255 个 C

32 位的 IP 地址可以用 4 个数字（小于 255）来表示，末位的 0 和 2 不能用于主机，255 用于广播地址。每个地址分为两个部分：网络地址和主机地址。网络地址，由相关组织分配，

代表了网段。A 类网络地址是使用最左边的一位字节作为网络地址编号，B 类网络地址是使用最左边的两位字节作为网络地址编号，等等。

为了简化网络管理，网络通常被划分为多个子网，用子网掩码来定义和识别子网的网段。在如果左边的三字节(24 位)用于区分不同的子网（网络地址），子网掩码是 11111111 11111111 11111111 00000000，用十进制表示为 255.255.255.0，使用无类域间路由选择(CIDR,classless interdomain routing)可表示为/24（使用掩码位）。使用掩码位的一个重要优点是能够将多个不相邻的地址集组合在单个子网内。例如，我们可以将若干 C 类子网组合为一个更大的子网分组。

IPv6 是一个 v4 的下一代协议，包括：

*更多的地址空间：IPv6 的地址是 128 位，支持 2 台主机。*增强的安全性（自带 IPsec）。*增强的质量服务（QOS）。

IPv6 的表示方法：

①冒分十六进制表示法

格式为 X：X：X：X：X：X：X：X，其中每个 X 表示地址中的 16b，以十六进制表示，例如：

ABCD：EF01：2345：6789：ABCD：EF01：2345：6789

这种表示法中，每个 X 的前导 0 是可以省略的，例如：

2001：0DB8：0000：0023：0008：0800：200C：417A→ 2001：DB8：0：23：8：800：200C：417A

②0 位压缩表示法（用：：表示 0）

在某些情况下，一个 IPv6 地址中间可能包含很长的一段 0，可以把连续的一段 0 压缩为“：：”。但为保证地址解析的唯一性，地址中”：：”只能出现一次，例如：

FF01：0：0：0：0：0：0：1101 → FF01：：1101；

0：0：0：0：0：0：0：1 → ：：1

0：0：0：0：0：0：0：0 → ：：

③内嵌 IPv4 地址表示法

为了实现 IPv4-IPv6 互通，IPv4 地址会嵌入 IPv6 地址中，此时地址常表示为：

X：X：X：X：X：X：d.d.d.d，前 96b 采用冒分十六进制表示，而最后 32b 地址则使用 IPv4 的点分十进制表示，例如：

：：192.168.0.1 与

：：FFFF：192.168.0.1 就是两个典型的例子。在前 96b 中，压缩 0 位的方法依旧适用。

考题中有出现 Teredo，即面向 IPv6 的 IPv4 NAT 网络地址转换穿越：在 IPv6/IPv4 主机位于一个或多个 IPv4 NAT 之后时，用来为单播 IPv6 连接提供地址分配和主机间自动隧道。为能够通过 IPv4 NAT，IPv6 数据包作为基于 IPv4 的用户数据包协议(UDP)消息发送出去。

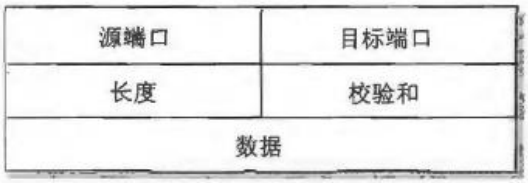
Teredo encapsulates IPv6 packets within UDP datagrams with IPv4 addressing. IPv6-aware systems behind the NAT device can be used as Teredo tunnel endpoints even if they do not have a dedicated public IPv4 address.

5.域名解析与寻址

网络上的地址有三个层次：底层的 MAC，中层的 IP，高层的域名；用到了 DNS、LDAP 什么

的。通过这些名字可以在网上定位和识别一个终端或客户端。它们都不安全，都可能被篡改。

TCP 格式



UDP 格式

图 6-13　与 UDP 相比，TCP 在其分片中携带更多的信息，因为它提供更多的服务

表 6-1　TCP 和 UDP 之间的主要差异

属性	TCP	UDP
可靠性	确保数据包到达其目的地，接收到数据包时返回 ACK，是一种可靠协议	不返回 ACK，不能保证数据包到达其目的地，是一种不可靠协议
连接	面向连接，因此进行握手，并且还与目标计算机建立虚拟连接	无连接，因此不进行握手，不建立虚拟连接
数据包排序	在首部内使用序列号，以确保传输的每一个数据包都被接受	并不使用序列号
拥塞控制	目标计算机能够告诉源计算机自己是否被淹没，从而降低传输速率	目标计算机不与源计算机就流量控制进行通信
用途	在需要可靠传送时使用。适合于传输相对少量的数据	在不需要可靠传送和需要传输大容量数据时(如视频流和状态广播)使用
速度与开销	使用相当多的资源，比 UDP 慢	使用较少的资源，比 TCP 快

6. 远程过程调用 RPC-Remote Procedure Call

RPC 是指跨主机执行对象的能力。工作在第五层，会话层。

7. Internet/Intranet/Extranet

- 互联网 Internet =外部不可信网络
- 内联网 Intranet =内部网络
- 外网 Extranet =外部不完全可信(例如，业务合作伙伴)

A.2 IP 网络连接

这里重点讲局域网 LAN。

LAN(局域网)技术存在三种主要类型：以太网、令牌环和 FDDI。CISSP 考试仅涉及这三种主要类型。LAN 技术之间的差别存在于数据链路层及其以下层（二层）。

1. 以太网 Ethernet

以太网基于 IEEE 802.3 标准，单独的以太网数据单元称为帧。以太网是一种共享介质的 LAN 技术，也称为广播技术。这意味着它准许很多设备在相同的介质上进行通信，但是要求每

台设备轮流通信并且执行冲突检测和避免操作。以太网采用广播域和冲突域。当两条被传输的消息企图同时使用网络介质时，就会出现数据冲突，这会导致其中一条或者两条消息出现。以太网可以支持全双工的通信,最常在星型或总线型拓扑上部署。以太网能够支持 100M 到 10Gbps 的速率（吞吐量）。

2.令牌环网 Token Ring

令牌环采用令牌传递机制来控制哪些系统可以在网络介质上传输数据。令牌在 LAN 所有成员形成的逻辑环上进行传递。令牌环可以采用环型或星型网络拓扑。由于令牌环的性能有限，比起以太网来成本又高，而且会增加部署和管理的难度，今天已极少使用。

令牌环可通过使用多站访问部件（MAU）配置为物理星形结构。

3.光纤分布式数据接口(FDDI) Fiber Distributed Data Interface

光纤分布式数据接口(FDDI)是一种使用两个环的高速令牌传递技术,其中信息流在两个环上沿相反的方向传输。FDDI 常用作大型企业网络的主干，它的双环设计允许实现自愈，即从环中去除故障网段,并且利用剩下的部分内部环和外部环建立单个环。虽然 FDDI 价格昂贵，但是在快速以太网和千兆以太网出现之前常常被用在校园环境中。价格稍便宜、距离有限且速度更慢的版本称为铜线分布式数据接口(CDDI)。CDDI 也更容易遭到干扰和偷听。

4.基础数据通信技术

①模拟通信与数字通信 Analog and Digital

使用频率、幅度、相位、电压等发生变化的连续信号时，就会进行模拟通信。连续信号的差异会产生一个波形(与数字信号的方被形成对照)。连续信号的差异实现实际通信。

通过使用非连续的电子信号以及状态改变或开关脉冲，就会出现数字通信。在长距离传输或存在干扰时，数字信号比模拟信号更可靠。

模拟和数字的区别很容易，如果以前没搞过通信，自己补补课。

②同步和异步 Synchronous and Asynchronous

同步通信依赖于定时或时钟机制，这种机制基于独立的时钟或数据流内嵌的时间标记。同步通信通常能够支持非常高速的数据传送。

异步通信依赖于停止和开始定界位来管理数据的传输。因为使用了定界位以及传输的停止和开始特征，所以异步通信最适用于较少量的数据。公用电话交换网(PSTN)调制器就是异步通信的一个绝佳示例。

同步速度快，异步速度慢。

③基带和宽带 Baseband and Broadband

在一个线缆段上能够同时发生的通信数取决于使用的是基带技术还是宽带技术。基带技术只能支持单个通信信道，它使用直流电应用于线缆，其中有电流表示二进制信号 1，无电流表示二进制信号 0。基带是一种数字信号形式。以太网线就是基带技术。

宽带技术能够支持多个同时发生的信号。宽带使用频率调制来支持许多信道，每个信道都支持一个截然不同的通信会话。宽带适用于高吞吐率，尤其适用于若干信道复用的情况。宽带是一种模拟信号形式。有线电视、线缆调制器、ISDN、DSL、T1 以及 T3 都是宽带技术的示例。

④介质访问 LAN Media Access

有五种局域网传输介质共享与冲突避免技术是比较重要的，即 LAN 介质访问技术，用来避

免或阻止传输冲突（必考）。

1.载波侦听多路存取(CSMA) Carrier-Sense Multiple Access/死等

1)主机侦听 LAN 介质，从而确定 LAN 介质是否正在使用中。

2)如果 LAN 介质未被使用，那么主机就传输其通信数据。

3)主机等待确认信号。

4)如果超时未接收到确认信号，那么主机从第一个步骤开始重新执行操作。

CSMA 不解决冲突，如果发生冲突，那么通信就不成功，因此也不会接收到确认信号。

2.有冲突避免的载波侦听多路存取(CSMA/CA) CSMA with Collision Avoidance/避免

1)主机有两个连接与 LAN 进行交互：通过入站（inbound）连接监听介质状态，通过出站连接（outbound）执行实际通信传输。第一步就是：主机侦听入站连接（inbound），确定 LAN 介质是否正在使用中。

2)如果 LAN 介质未被使用，那么主机就请求传输特权。

3)如果超时之后仍未获得特权，那么主机从第一个步骤开始重新执行操作。

4)如果被授予特权，那么主机就通过出站连接传输其通信数据，不过也要先发送通信请求 SYN 给接收端，等回应后和建立通信会话。

5)主机等待确认信号 ACK，有则通，没有则断。

6)如果超时之后仍未收到确认信号，那么主机从第一个步骤开始重新执行操作。

Apple Talk 和 802.11 无线网络连接是利用 CSMA/CA 技术的网络例子。CSMA/CA 系统要求指定一个主系统，这个系统能够响应请求以及授予发送数据传输的特权。

3.有冲突检测的载波侦听多路存取(CSMA/CD) CSMA with Collision Detection/检测

1) 主机侦听 LAN 介质，从而确定 LAN 介质是否正在使用中。

2) 如果 LAN 介质未被使用，那么主机就传输其通信数据。

3) 在数据传输的同时，主机侦听冲突(也就是其它主机同时传送数据的情况)。

4) 如果检测到冲突，那么主机就会传输一个停发信号。

5) 如果接收到停发信号，所有主机都会停止数据传输。每台主机都会等待一个**随机**的时间周期，然后从第一个步骤开始重新执行操作。

以太网利用了 CSMA/CD 技术。通过使冲突域的每个成员在重新开始传输过程之前都进行随机的短时间等待， CSMA/CD 可以响应冲突。不过，准许冲突发生以及随后对冲突的响应或反应会导致传输延迟以及要求重复传输，这会导致损失百分之四十左右的潜在吞吐量。

4.令牌传递 Token Passing

持有令牌的主机有权传输数据。一旦传输完成，主机就会将令牌释放给下一个系统。令牌传递用在令牌环网络中。（令牌永远不会有冲突，但复用效能差，所以用多个环）

例如 FDDI：它是 100M 的骨干网络，只有一个主环被使用，另一个环是备份环；两个环的方向相反；环也被称为计数器旋转。

5.轮询 Polling

这是一种使用主从配置进行通信的 LAN 介质访问技术。一个系统被标记为主系统，其他所有系统则被标记为从属系统。主系统依次轮询或了解每个从属系统是否需要传输数据。如果某个从属系统表明了这种需求，那么就会被授予传输数据的特权。一旦该系统的传输结束，主

系统就继续轮询下一个从属系统。同步数据链接控制(SDLC)就使用了轮询。

轮询通过使用许可系统来解决冲突。轮询是 CSMA/CA 方法的逆过程。虽然二者都使用主从结构，但是 CSMA/CA 允许从系统请求特权，而轮询则由主系统提供特权。轮询可以被配置为授予某个(或多个)系统具有比其他系统更高的优先权。例如，如果标准的轮询模式为 1、2、3、4.那么就可以指定系统 1 优先，轮询模式相应会变化为 1、2、1、3、1、4。

6.路由协议

路由器提供了异构网互联的机制，实现将一个网络的数据包发送到另一个网络。路由协议就是用来规范 IP 数据包发送过程中寻找目的的规定和标准。

自治域 AS（autonomous systems），独立的广域网。

①静态路由 static，自动发现和维护路由表。

②动态路由 dynamic，手动配置路由表。

IGP 内部网关协议

有 IS-IS，IGER，EIGER 等 。

1.距离向量协议 destination metric：使用跳数或向量来确定最短距离。如路由信息协议 RIP（Routing Information Protocol）

2.链路状态协议 link-state：不考虑跳数，使用“图形理论”算法或最短路径优先算法，有更短的收敛时间，支持 VISM(可变长子网掩码)和 CIDR。如开放最短路径优先协议 OSPF（Open Shortest Path First）。

3.开放最短路径优先(OSPF)

OSPF 协议是一种基于最短路径优选和链路状态算法的网络层路由协议。路由器使用链路状态算法通告发送路由信息给网络内的所有节点，各节点使用最短路径信息计算到其他每个节点的最优拓扑。每个路由器发送部分的路由表(路由到部分网络目的地的信息)描述自己的链路状态，有的时候也并发送完整的路由结构(拓扑)。最短路径算法的优点是，使用较小的 LSA 信息进行更频繁的更新。它们收敛很快，从而防止路由环路问题，避免计数到无穷大(对于一个特定的网络，路由器的跳数不断增加)。最短路径算法的缺点是，它们需要大量的 CPU 能力和内存空间。

EGP 外部网关协议

已经过时的路由协议。常用的有：

BGP（Border Gateway Protocol）：一种高级的距离向量路由协议。

A.3 多层协议的含义（例如：DNP3）

DNP3 是 CISSP 考试的内容之一，主要用于电力和水利行业的使用和管理，支持数据采集系统和系统控制设备之间的通信（工业控制系统 SCADA）。它包含子站计算机、RTU(远程终端单元/通过嵌入式微处理器控制设备)、IED(智能电子设备)和 SCADA 主站(即控制中心)。DNP3 是一个开放的公共的标准，**不提供安全性**，是个多层协议且功能类似 TCP/IP。

多层协议和聚合协议是两个相关联的概念，没必要严格区分，分层协议有些固有的优点：

1.高层可使用更为广泛的协议；2.通过封装在不同层进行合作；2.灵活和弹性。

分层架构也有缺点：

1.存在隐蔽信道；

2.过滤机制可被绕行；

3.逻辑网络段边界可以被逾越；

4.协议栈漏洞、数据不安全、会话劫持/中间人攻击、操作系统与服务的弱点，设备后门。

A.4 聚合协议（例如：FCoE,MPLS,VoIP,iSCSI）

聚合协议也称为汇聚协议/融合协议（Converged Protocols），一个融合多层的网络基础设施，也就是 IP 聚合（IP Convergence），可以带来以下好处：

①对多媒体应用的良好支持。

②一个 IP 融合网络是一个支撑多种创新应用交互的独立平台。

③融合 IP 网络更易于管理，因为系统资源设置可以统一设置。

④一个需求较少网络组件的统一环境。

典型应用就是传统的自动电话交换网（电路交换）已经从所谓的软交换过渡到融合通信了。

1.以太网光纤通道(FCoE) Fibre Channel over Ethernet

以太网光纤通道(FCoE)是网络存储解决方案（存储区域网络 SAN 或网络附加存储 NAS）的一种形式，一个轻量级封装协议，缺乏 TCP 层的可靠数据传输，它允许高达 16Gbps 的上行高速文件传输。通过这一技术，光纤通道作为一个网络层或 OSI 第三层协议，替换 IP 作为一个标准的以太网网络负载（一、二、三层都融合在一个光纤通道上）。FCoE 必须使用 DCB-enable 模式的以太，并使用无损通信保证级别，不使用 TCP 或 IP 协议是一个 2 层（非路由）协议，仅支持一个数据中心内的短距通信。DCB 是指数据中心桥接标准。

2.MPLS（多协议标签交换）Multiprotocol Label Switching

MPLS 是一个广域网协议，是一种高通过、高性能的网络技术，它将数据在网络中以基于最短路径的标签而不是更长的网络地址进行传输。这种技术节省了传统的基于 IP 的路由过程，这个过程可能是相当复杂的。此外，MPLS 可以封装处理更广泛的协议，不局限于 TCP/IP，包括 T1/El、ATM、帧中继、SONET 和 DSL 等。

3.IP 语音（VoIP）Voice over IP（考点）

是用于在 TCP/IP 网络传输语音/视频/数据的一种隧道机制，可以取代 PSTN。VoIP 系统是基于会话发起协议(SIP)的使用，这是公认的标准。任何 SIP 兼容设备可以彼此通信。VoIP 也存在一些问题：

①丢包：通过数据包丢失隐藏(PLC)的技术，掩盖丢包的影响。有几种实现方法：一是零替代，最简单，用空值替代丢失的包；二是间隙插值，就是线性插值计算来填充。

②抖动：抖动导致通话延迟，但不完全是因为网络延迟原因造成的，可通过增加数据包缓冲区大小来补偿抖动。

③顺序错误/序列误差：顺序错误导致通话质量恶化通常，因为经过路由的网络数据包可能以不同的顺序到达目的。

SIP 协议 Session Initiation Protocol（会话发起协议）用来处理多媒体连接，通过 MD5 哈希提供完整性保护。

4.互联网小型计算机系统接口（iSCSI）

互联网小型计算机系统接口(iSCSI)是一个基于 IP 的网络存储标准。这项技术可以用来支持位置独立的文件存储、传输和局域网、广域网的检索，或者公共互联网连接。iSCSI 常被认为是光纤通道(FCoE)的一种低成本替代。

A.5 软件定义网络

1.软件定义网络(SDN) Software-Defined Networking

SDN 基于这样一个现实情况，即传统网络设备配置的复杂性(如路由器和交换机)经常强迫组织依附于一个单一的设备厂商，如思科，限制了网络的灵活性难以应对不断变化的物理和商业条件。SDN 移除了 IP 寻址、子网、路由以及诸如此类繁杂的数据通信技术。SDN 通过高效的网络虚拟化，提供了一种直接从中央位置进行新网络设计的方法，它是灵活的、与厂商无关的、可并且是基于开放标准。利用 SDN 使得组织可以不从单一供应商采购设备。相反，它允许组织混合和匹配需要的硬件，如选择最划算的或最高通过性能的设备而不管其供应商是谁。之后，通过集中管理接口进行配置和管理硬件控制。此外，在硬件上的应用设置可以根据需要动态地进行变更和调整。SDN 旨在把控制层(即网络服务的数据传输管理)和基础设施层(即硬件和基于硬件的设置)分离。也就是把网络分为三层（控制与数据分离），有 2 类接口：

①控制层(控制平面)：SDN 控制器包括一个或多个 NBI（北向接口）代理、SDN 控制逻辑和并控制数据平面接口(CDPI)驱动程序。

②应用层(应用平面)：SDN 应用程序通过北向接口(NBI)与 SDN 控制层面进行通信。一个 SDN 应用程序由一个 SDN 应用逻辑和一个或多个 NBI 驱动器构成。它的功能就是执行和实现上层的控制指令，满足应用的网络需求。

③基础设施层(数据平面)：SDN 数据通路是一个逻辑网络设备，包括 CDPI（SDN 控制数据平面接口）代理和一组一个或多个流量转发引擎和零个或多个业务处理功能。

两类接口：

①SDN 控制数据平面接口(CDPI)：SDN CDPI 定义 SDN 控制器和一个 SDN 数据通路之间的接口，它提供了所有的转发操作，编程控制功能的通告，统计报告和事件通知。

②SDN 北向接口(NBI)：是 SDN 应用层与控制器之间的通信接口，表达和传递网络的行为及需求。北向是上层的，管理的；南向是下层的，操作的。

A.6 无线网络

1.各种无线网络通信标准

802.11 泛指整个协议簇，也指第一个无线协议，反正有好多标准，必考：

①802.11： 2.4G, 2M, WEP
801.11b： 2.4G, 11M, DSSS（直接序列扩频），有 14 个 22Mhs 频宽的频道，兼容
802.11e： 2.4G,提供 QOS
802.11f： 2.4G,支持 AP 漫游（IAPP 协议）
802.11g： 2.4G, 54M(物理层)24M(传输层)，兼容，OFDM(正交频分)
低频 2.4G 的 Befg 记忆：小蜜蜂飞机
③802.11a： 5G, 54M(物理层)24M(传输层)，OFDM(正交频分)，短距，美国用，不兼容

802.11h： 5G，用于欧洲

802.11n：2.4G&5G， >275M，MIMO（多入多出），4 天线，20MHz 频宽，兼容

802.11ac：5G，1000M

高频 5G 的 Ahnac 记忆：A-hn-AC，爱湖南菜，标准 n 是双频的。

④802.11j： 多标准集成，为了适应日本的 5G 频率标准。（J 就是搞 Japan）

⑤802.16： MAN（无线城域网），WiMAX（小灵通，6M~30M）（记忆：16 比 15 大）

802.15： WPAN（无线个人局域网），蓝牙，2.4G，3Mbps，10 米（33 英尺）

⑥802.11i：针对 802.11 的 WEP 安全问题，定义了基于 AES 的 CCMP 协议，支持 WPA2

⑦802.1x：不只是针对无线网，它就是一套独立的用于认证的协议。

2.无线网络组网通信的几种模式

1.基础设施模式 infrastructure mode

需要一个网络接入点 **AP！**

①独立模式 stand-alone：1 个 AP 的无线局域网，不外联。

②有线扩展模式 wired extension：通过 AP 接入有线网。

③企业扩展模式 enterprise extended：广域到处都有很多 AP，它们属于同一个公司用同一个扩展服务集标示符 ESSID，接入同一个有线网。

④桥接 bridge：连接 2 个有线网，起桥接作用。

2.点对点模式 ad hoc mode

终端直接通信，没有 AP。

3. SSID 服务集标示符 service set identifier

SSID 通常用来表示一个无线网络的名称。有 2 种类型：

①扩展服务集标识符 ESSID。是使用无线基站或 WAP 的无线网络名称。

②基本服务集标识符 BSSID。是使用 adhoc 或点对点模式时无线网络的名称。然而，在基础设施模式下运行时， BSSID 拥有 ESSID 基站主机的 MAC 地址，用于区分一个扩展无线网络中的多个基站。

SSID 最好关闭，以提高安全性。

4.无线网状网络 Wireless Mesh Network (WMN)

由无线节点组成的一个网状拓扑，每个节点可以替代转发，可以自愈。

Ad-hoc 网络和无线 Mesh 网络都采用分布式、自组织的思想形成网络，网络每个节点都具备路由功能，随时为其他节点的数据传输提供路由和中继服务。但是：

Ad-hoc 网络主要侧重应用于**移动**（运动）环境中，数据流可以包括语音、数据和多媒体信息；是一种多跳的、无中心的、自组织无线网络，又称为多跳网（Multi-hop Network）、无基础设施网（Infrastructureless Network）或自组织网（Self-organizing Network）。整个网络没有固定的基础设施，每个节点都是移动的，并且都能以任意方式动态地保持与其它节点的联系。在这种网络中，由于终端无线覆盖取值范围的有限性，两个无法直接进行通信的

用户终端可以借助其它节点进行分组转发。每一个节点同时是一个路由器，它们能完成发现以及维持到其它节点路由的功能。

无线 Mesh 网络是一种无线宽带**接入**网络，让用户在任何时间、任何地点都可以接入互联网进行高速无线访问。

无线 mesh 网络，由 mesh routers（路由器）和 mesh clients（客户端）组成，其中 mesh routers 构成骨干网络，并和有线的 internet 网相连接，负责为 mesh clients 提供多跳的无线 internet 连接。 无线 Mesh 网络（无线网状网络）也称为“多跳（multi-hop）”网络，它是一种与传统无线网络完全不同的新型无线网络技术。

3.无线网络的加密和安全（必考）

最早的 802.11 标准基本上是不安全的。IEEE 802.11 标准定义了两种无线客户端向无线接入点进行验证的方法：开放系统认证(OSA)和共享密钥认证(SKA)。OSA 是不认证的，连上就通信，而且纯明文传输；SKA 要求身份验证，可选用 WEB、WPA、WPA2 等验证技术。

先总结一下：

WEP：64/128 位密钥，RC4 对称流加密，使用初始向量。

WPA：64/128 位密钥，RC4 对称流加密，MIC（消息完整性检查），TKIP+RADIUS

WPA-PSK：64/128 位密钥，RC4 对称流加密，MIC（消息完整性检查），TKIP+PSK

WPA2：128 位密钥，AES，MIC（消息完整性检查），CCMP+RADIUS

WPA2-PSK：128 位密钥，AES，MIC（消息完整性检查），CCMP+PSK

①WEP 有线等效保密协议/有线等效私密性协议 Wired Equivalent Privacy

WEP 使用一个静态的公共密钥和使用脆弱的 IV(初始向量)，不到 60 秒就可以破解 WEP。流密码基于共享密钥，产生密钥流，即伪随机比特序列，和一个初始化向量(IV)。密钥对明文进行异或运算后产生的密文。流密码的一个重要特性是，如果明文和密文的密钥流序列是已知的，密钥可以通过简单的异或明文和密文恢复（已知明文、密文攻击），恢复的密钥可以被攻击者用来加密的挑战文本的任何后续的访问点生成的异或值加在一起，产生一个有效的认证响应。因此，攻击者可以通过访问点的身份验证。

②Wi-Fi 保护访问（WIFI 网络安全存取）WPA/ Wi-Fi Protected Access

替代 WEP，直到 802.11i 修订完成，又被 WPA2 取代。

Wi-Fi 访问保护是基于 LEAP 和 TKIP（临时密钥完整性协议）加密体系的基础上并对认证过程进行加密。使用之前介绍的 802.1x 认证协议，来进行用户身份认证。如果使用单个静态的密码，仍有可能被暴力破解。

③WPA2（WIFI 网络安全存取 2）

它的原理和 WPA 其实是完成不同的，使用了计数器模式的密码块链接消息认证码协议(CCMP) Counter Mode Cipher Block Chaining Message Authentication Code Protocol，这基于 AES 的加密方案，目前还没有被破解的案例。

④802.1X/EAP（必考）

802. 1X 是无线网络利用现有的网络基础设施进行认证服务的协议，包括多种技术解决方案，如 RADIUS、TACACS、证书、智能卡、令牌和生物识别设备笔。802.1X 可以实现客户端没

有得到入网允许，没有得到 IP 地址前，将用户 MAC 地址信息和符合信息传输到服务器进行验证，通过了就可以分配 IP 让客户端入网了。也就是路由器要支持 802.1X。但是在发送身份信息过程中可能被劫持什么的，所以它还要附加一些加密的协议和功能。

EAP(可扩展认证协议) Extensible Authentication Protocol 是一个认证框架而不是一个具体的认证机制，允许采用各种新的认证技术与现有技术兼容。有超过 40 种不同的 EAP 认证方法获得广泛地支持，如：LEAP，EAP-TLS，EAP-SIM，EAP-AKA 和 EAP-TTLS。其中，有些比较老的技术已经被破解了，如：EAP-MD5。

802.1X/EAP，被称为企业认证，就是一个标准的基于端口的网络访问控制协议，确保客户端在没有发生正确认证时不能和资源发生通信。

WEP、WPA 和 WPA2 都支持 802.1X/EAP。

⑤PEAP 受保护的可扩展认证协议 Protected Extensible Authentication Protocol

EAP 最初被设计用在相互物理隔离通道，是不加密的。于是 PEAP 用来为 EAP 提供加密，它利用 TLS 隧道封装 EAP。

⑥LEAP 轻量级可扩展认证协议 Lightweight Extensible Authentication Protocol

LEAP 是 Cisco 专有的认证协议，用于 WPA，可替代 TKIP。它并不安全，2000 年就破解了。

⑦MAC 过滤器 MAC Filter

MAC 过滤可以防止蹭网，不过大规模无线局域网管起来有点麻烦，主机太多了，而且 MAC 很容易被伪造。

⑧TKIP 临时密钥完整性协议 Temporal Key Integrity Protocol

TKIP 用于 WPA，可替代 WEP，且不需要更换无线硬件，它在使用 RC4 算法密钥进行加密之前结合了初始向量(IV)与安全的根密钥；一个序列计数器被用来防止报文重放攻击；同时还使用 Michael 进行完整性检查。TKIP 后来又被 CCMP 替代了。

⑨CCMP 密码块链消息认证码协议计数器模式 Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CCMP 用于取代 WEP 和 TKIP/WPA，它使用 AES (高级加密标准)和一个 128 位的密钥。

总体过程：WEP　WPA=SKIP+LEAP　WPA2=CCMP，

4.天线 Antenna

天线要设置在合适的位置，哪个位置好自己看风水。天线有很多种，要知道它们的名字。

5.蓝牙 IEEE 802.15

蓝牙更趋向于本地使用，其目的是“更换连接设备的电缆”，其最大范围为 100 米(330 英尺)，使用 2.4GHz 频率，主要用于工业环境，使用 4 位 PIN 码来配对。范围取决于该设备的使用功率等级。在蓝牙网络中，通常使用 2 级，范围可达 10 米(33 英尺)，这个速度足够传送高保真音乐传输和视频流。针对或利用蓝牙的攻击有 2 种。

①**Bluesnarfing**：目的是窃密。targets the data on luetooth-enabled devices.

②**Bluejacking**：目的是广告。send unsolicited messages via Bluetooth.

6.全球微波互联接入

无线宽带的一个著名的例子是 WiMAX。通过 WiMAX 技术，可以提供超过 30 兆位/秒的数据

速率，但供应商提供 6Mbps 或更少的平均数据速率，这使服务速率比有线宽带明显减慢。

7.无线基础知识

前面讲了很多无线网络的内容，现在回过头来讲讲无线通信。频谱资源是有限的，900M，2.4G，5GHz 的频率是公开的，很多设备都用这几个频段。怎么避免频率冲突和干扰呢？必须使用频率复用的技术。

①扩频 Spread spectrum。指的是通信可以通过多个频率同时发生。因此，一条报文可以被分为若干片段，所有片段同时进行发送，不过每个片段都使用不同的频率。实际上，这是一种并行通信，而不是串行通信。

②跳频扩频(FHSS)。是扩频概念的早期实现。然而，这种技术并非以并行方式发送数据，而是串行传输数据，同时不断改变所使用的频率。可用频率的整个范围都会被使用，但是每次只使用一个频率。发送者改变频率时，为了接收到信号，接收者必须遵循相同的跳频模式。FHSS 被设计用于帮助最小化干扰，而不是只使用会受到影响的单一顿率。在实际使用中，通过不断切换频率，干扰就被最小化。

③直接序列扩频(DSSS)。以并行方式同时利用所有可用频率。与 FHSS 相比，DSSS 提供了更高的数据吞吐率。DSSS 也使用被称为碎片码的特殊编码机制来允许接收方重构数据，即使是部分信号由于干扰被破坏也同样适用。这种情况与 RAID-5 的奇偶位允许重新创建所丢失驱动器上数据几乎完全相同。

④正交频分复用(OFDM)。仍然是另一种频率使用的变化形式。OFDM 利用了允许传输进行更紧密压缩的数字多载波调制模式。已调制信号是正交的，因此不会导致相互干扰。最后，OFDM 需要的频率组(也就是信道频宽)更小，却能够提供更大的数据吞吐率。

蜂窝电话从 1G 发展到 4G，大家应该都比较清楚了，不详说。

1G：NMT、AMPS、TACS；

2G：GSM、iDEN、TDMA、CDMAPDC；

2.5G：HSCSD、GPRS；

3G：W-CDMA、TD-CDMA、UWC、EDGE、DECT、UMTS；

4G：WiMax - IEEE 802.16、XOHM (Brand name of WiMax)、Mobile Broadband - IEEE 802.20、LTE (Long Term Evolution)

A.7 用于维护通信安全的密码学

密码学看第三域，I 章节。

1.如何使用证书

安全专家需要确保他们熟悉最常用的五种产品证书（都是 PKI 提供的证书）：

①客户端 SSL 证书。用来确定客户端与服务器端的 SSL(客户端身份验证)。例子：一个银行给顾客一个客户端的 SSL 证书，允许银行的服务器来识别客户和授权访问客户的账户。

②服务器端 SSL 证书。用来识别服务器到客户端的 SSL(服务器身份验证)。服务器可以使用或不使用客户端认证。在使用加密的 SSL 会话时候，服务器端认证是一个基本要求。例如：从事电子商务的互联网网站，通常支持基于服务器身份验证证书，至少，要建立一个加密的 SSL 会话，基于此向消费者保证，与他们所交易的网站是一个经过认证的特定公司站点。加密

的 SSL 会话可以保证，在网络传送的个人信息(如，信用卡号码)不被轻易的截获。

③S/MIME 证书。用于签名和加密的电子邮件（使用 PKI）。与客户端的 SSL 证书，客户端的身份通常被认为是作为一个人类的身份，如一个企业的员工。一个单一的证书可以作为双方的 S/MIME 证书和 SSL 证书。S/MIME 证书也可用于表单签名，和一个单点登录解决方案的一部分。例子：一个公司部署结合 S/MIME 和 SSL 证书仅用于验证员工身份的目的，从而允许签名的电子邮件客户端 SSL 认证，但不加密的电子邮件。另一家公司使用 S/MIME 证书用于双方签名和加密电子邮件，起到处理敏感的财务或法律事务处理的目的。

④对象签名证书。用于识别程序代码签名者，签名脚本，或其他的签名文件。例如：一个软件公司对一个发布在互联网上的软件进行签名，为用户提供了软件公司合法产品的保证。以这种方式使用证书和数字签名，也可以让用户识别和控制下载合法软件倒自己的电脑上。

⑤证书颁发机构/权威认证机构(CA)证书，用于识别 CAs。客户端和服务器软件使用 CA 证书来确定什么样的其他证书是可信的。例如：CA 证书存储在一个程序或应用程序中，确定哪些证书是可以验证程序的副本。管理员可以通过控制每个用户 CA 证书副本存储在应用程序，来实现公司安全政策的某些形势。

2.证书和轻量级目录访问协议(LDAP)目录

在一个组织中，使用 LDAP 访问目录服务支持极大灵活性的证书管理。在 LDAP 兼容的目录管理中，系统管理员可以存储多种需要的证书信息。LCAP 就是存储、管理、分发证书的东西。

B.保护网络组件安全

这里讲主要的网络安防手段和措施。

了解下 2 种欺骗：

①非盲欺骗（不与主机通信）

这种类型的攻击发生时，攻击者和受害者在相同的子网内，攻击者只监测数据，而不拦截数据。在这种情况下，欺骗的最大威胁是会话劫持。这是通过欺骗一个建立连接的数据流来完成的，之后，攻击者重新建立基于正确的顺序号和确认号的通信。

②盲欺骗（与主机进行通信）

这是一个更复杂的攻击。几个数据包被发送到目标主机，为了获取序列号样本并最终检测正确顺序。如果序列号被地露，数据可以被发送到目标主机。

B.1 硬件操作（例如：调制解调器、交换机、路由器、无线接入点、移动设备）

这里介绍各种网络设备，都是常用的，不难。不过要熟悉通信和交换的原理。

1.冲突与广播 Collisions vs. Broadcasts

①当两个系统同时在 1 个通信信道或传输介质上传送数据时，就会发生冲突。

②当单个系统向所有可能的接收者发送数据时，就会发生广播。

冲突避免技术是各种网络设备必须要采用的，即如何管理冲突域和广播域。使用任何第二层或更高层设备可以分割冲突域，使用任何或更高层设备则可以分割广播域。域被分割时，就意味着部署在设备另一侧上的系统是不同域的成员。

①中继器、集中器和放大器 Repeaters, Concentrators, and Amplifiers（一层）

工作在 OSI 模型的第一层，设备两侧的系统都位于相同的冲突域和广播域内。

*集中器连接多个连接设备，在网络上一个信号传送。例如，一个光纤分布式数据接口(FDDI)集中器将传输连接设备到 FDDI 环。

②集线器 Hubs（一层）

集线器用于连接使用相同协议的网段，它们将入站通信在所有出站端口上进行中继，也就是一种多端口的中继器。在 OSI 模型的第一层上工作。集线器两侧的系统都位于同一冲突域和广播域内。集线器是一种过时的技术，交换机已替代它们。

*集线器传输每个端口信号到其它所有端口，实现了一个物理星形拓扑结构，有很多缺点。

③调制解调器 Modems

在模拟信号和数据信息之间进行调制，从而在公共电话网络(PSTN)等模拟线路上进行数据通信。最早的 56K 模拟猫已经被 ISDN、DSL 调制解调器，电缆调制解调器、802.11 无线以及各种形式无线调制解调器的数字宽带技术所替代。其实被称为调制解调(电缆、DSL、ISDN、无线等)的现代设备是路由器而不是纯粹的调制解调器。

④桥 Bridges（二层）

桥将两个异构的网络(拓扑结构、线缆类型和速度不同的网络)连接在一起，以便连接使用相同协议的网段。桥将通信从一个网络转发至另一个网络。将使用不同传输速率的网络连接在一起的桥可以缓存数据包，直至这些数据包被转发至较慢的网络，这称为存储转发设备。桥在 OSI 模型的第二层上工作，基于 MAC 地址。桥两侧的系统位于相同的广播域内，不过所在的冲突域不同。

⑤交换机 Switches（二层）

交换机知道每个出站端口上所连接系统的地址，能够更有效地流量传递、建立隔离的冲突域以及提高数据的总体吞吐量。在用于创建 VLAN 时，交换机也可以创建隔离的广播域。交换机主要在 OSI 模型的第二层上工作，用于连接使用相同协议的网段，两侧的系统位于同一广播域内，不过冲突域不同。一个交换机的每端口都是一个冲突域，使用 CSMA/CD 逻辑传输机制，能够更有效率的在以太网络中传输。

如果是三层交换机，原理等同于路由器，两侧的系统位于不同的广播域和冲突域内。

⑥路由器 Routers

路由器用于控制网络上的通信流，在 OSI 模型的第三层上工作，用于连接使用相同协议的网段，两侧的系统属于不同的广播域和冲突域。动态的路由协议有：RIP、OSPF 和 BGP。还有一种叫做桥式路由器（Brouters）的东西，我没见过。如果路由失败，那么就默认进行桥接。

⑦网关 Gateways

网关能够连接使用不同网络协议的网络。通过将通信的格式转换为与每个网络采用的协议或传输方法都兼容的形式，网关就可以负责从一个网络向另一个网络传输通信信息。网关也称为协议转换器，既可以作为独立硬件设备，也可以作为一种软件服务(例如 IP-to-IPX 网关)。网关两侧的系统位于不同的广播域和冲突域内。网关具有很多类型，包括数据、邮件、应用、安全和互联网。网关通常在 OSl 模型的第七层上工作。

B.2 传输介质(例如：有线、无线、光纤)

1.同轴电缆 Coaxial Cable

同轴电缆的设计使其能够完全抵抗电磁干扰(EMI) electromagnetic interference，能够支持高带宽(对比同时代的其他技术)，并且提供比双绞线更长的可用长度。由于双绞线更加低廉的成本且安装简便，它最终失去了其主导地位。同轴电缆的两端（末端）需要使用网段终结器（50 欧姆电阻器）（2000 年以前读大学的，宿舍局域网都用过同轴网卡）。

①细缆/细同轴，也被称为 10Base2，通常用来将系统连接到粗缆主干线路。细缆可以扩展到 185 米的距离，并且能够提供高达 10Mbps 的吞吐率。

②粗缆/粗同轴，也被称为 10Base5，可以扩展到 500 米的距离，能够提供高达 10Mbps 的吞吐率。

2.基带和宽带线缆 Baseband and Broadband Cables

10Base2 线路中的 Base，就是表示线路的基带或宽带特性；10 代表速率，2 代表距离。基带线缆一次只能够传输一个单独的信号，宽带线缆则可以同时传输多个信号。绝大多数网络连线都采用基带线缆。然而，在特定的配置中使用时，同轴电缆可以被用作宽带连接，例如线缆调制解调器。

3.双绞线 Twisted-Pair

有屏蔽层的双绞线被称为屏蔽双绞线（CTP）shielded twisted-pair，反正为非屏蔽双绞线（UTP）。线缆的缠绕可以使线缆免受外部的无线电频率、电子和磁性干扰，并且降低了线对之间的串扰。缠绕得越紧(每英寸进行的缠绕越多)，那么对内部和外部干扰以及串扰的屏蔽也就越强，因此吞吐的能力也就越大(也就是说具有更大的带宽)。长度不超 100 米。

各类双绞线的速度也要搞清楚，懒得列出来了。（七类万兆，超五、六类是千兆）

4.铜导线 Conductors

铜导线存在电阻，这使得信号的强度和质量在超出线缆的长度时会降低。信号的这种降低被称为衰减attenuation。阻燃线缆是一种用燃烧时不会释放毒烟的特殊材料包围的线缆连接，就像传统的 PVC 覆盖布线。

5.光纤

单模：该模式具有小直径芯，减少电缆内光反射的次数。这可以有更大的传输距离，达到 80 公里，是多模光纤的 50 倍还多。

多模：这种模式使用比单模有更大直径的电缆。随后，增加光的反射。通常用于短距离。传输距离可达 400 米。

塑料光纤(POF)：采用塑料芯和允许较大直径的纤维芯。信号失真是由于塑性大大增加，这明显的限制了它的范围。传输距离约 100m。

B.3 网络访问控制设备（例如：防火墙、代理服务器）

1.防火墙 Firewalls

防火墙被用于阻止或过滤通信，可以基于内容、应用、协议、端口或源地址来阻止已知的恶意数据、消息或数据包，能够对公共网络隐藏专用网络的结构和寻址方案，并提供日志记录、审计和监控性能以及警报和基本的入侵检测系统（IDS）功能。TCP_Wrapper 软件包是一种基于 TCP/IP 协议之上的、运行于 UNIX/Linux 系统、基于访问控制技术的一种网络防火墙软件。

防火墙分类是很基础的知识，必考：

①静态的数据包过滤防火墙 Static Packet-Filtering Firewalls（第一代）(第三层)

检查 IP 报文头部的数据进行通信的过滤。过滤规则基于于源地址、目的地址和端口地址。静态过滤防火墙不提供身份验证，不区分数据包来源，来自专用网络内部还是外部。这种防火墙也被称为屏蔽路由器或常用路由器。

②应用级网关(代理)防火墙 Application-Level Gateway Firewalls（第二代）(第七层)

应用级网关防火墙也称为代理防火墙，基于用于传送或接收数据的网络服务(也就是应用)来过滤通信。每种应用类型都必须具有其自己的唯一代理服务器。因此，应用级网关防火墙包括很多独立的代理服务器。由于每个信息数据包在通过防火墙时都必须经过检查和处理，因此这种类型的防火墙性能不高。应用级网关在 OSI 模型的应用层(第七层)上工作。

③电路级网关（代理）防火墙 Circuit-Level Gateway Firewalls（第二代）(第五层)

电路级网关防火墙也称为电路代理，用于在可信合作伙伴之间建立通信会话，它在 OSI 模型的会话层(第五层)上工作。SOCKS (来自安全套接字，就像 TCP/IP 端口一样)是电路级网关防火墙的通用实现。相当于信道加密。这种防火墙只基于通信电路的终点名称(也就是源地址、目的地址以及服务端口号)来许可或拒绝转发决策。它仍被视为第二代防火墙。

④状态检测防火墙 Stateful Inspection Firewalls（第三代）(第四层)

状态检测防火墙也被成为动态包过滤防火墙，要对网络通信的状态或环境进行评估。通过查看源和目的地地址、应用习惯、起源地以及当前数据包与同一会话先前数据包之间的关系，状态检测防火墙就能够为已授权的用户和活动授予广泛的访问权限，并且能够积极地监视和阻止未授权的用户和活动。状态检测防火墙通常比应用级网关防火墙更为有效。状态检测防火墙被视为第三代防火墙，并且在 OSI 模型的网络层和传输层(第三、四层)上工作，即网络层过滤，会话层和应用层检查。

2.多宿主防火墙 Multihomed Firewalls

防火墙一般都具有多个接口(具有两个接口的防火墙被称为双宿主防火墙)。其实要 1 对接口才能串接进网络，2 对接口可以管控 2 个子网。不过，这 2 个子网必须隔离，不能在防火墙内实现数据交换。

堡垒主机/屏蔽主机 bastion host /screened host

位于专用网络和不可信网络之间的防火墙系统（边界设备），通常位于外联路由器之后。堡垒主机不仅负责过滤进入专用网络的通信，而且还负责保护内部客户端的身份。术语"堡垒"来源于中世纪的城堡建筑风格，其中堡垒警戒室位于主入口前面，也就是现在的门户岗亭。

利用堡垒主机(Bastion Host)和一台包过滤路由器构建，堡垒主机处于内网中提供代理服务，包过滤路由器除提供过滤功能外，还被配置为只允许堡垒主机进行外部访问，所以内部主机只能通过堡垒主机代理访问外部网络，安全性较高。

屏蔽子网 screened subnet

屏蔽子网与屏蔽主机(也就是堡垒主机)在概念上相似，是指包含堡垒主机的，位于外网、内网两个路由器之间，1 个子网。是内部系统外联的一个代理区。

DMZ

就是屏蔽子网，是个网络隔离区（停火区/非军事区）。能够访问外网、内网，与外网、

内网间都有隔离手段。DMZ 常常是公共 Web、电子邮件、文件以及其他资源服务器的宿主。

3.防火墙的部署

①单层部署。只提供最低限度的保护，很简单。

②双层部署。使用多个防火墙，分别联外网、内网，形成一个 DMZ。中等安全。

③三层部署。在 DMZ 以内，再部署防火墙，区分不同等级的事务处理子网。太复杂了。

4.防火墙策略类型

①静默规则（要少日志）：不记录任何被过滤流量的日志，减少系统日志大小。

Silent rule,Drops “noisy” traffic without logging it. This reduces log sizes by not responding to packets that are deemed unimportant.

②安全规则（要严登陆）：严格限定登陆和配置防火墙的终端设备，禁止未授权访问。

Stealth rule,Disallows access to firewall software from unauthorized systems.

③消除规则（最后一条）：配置在防火墙规则库（策略库）的最后一条，过滤所有不符合前述规则的流量，并记录相关日志。

Cleanup rule,The last rule in the rule base, which drops and logs any traffic that does not meet the preceding rules.

④限制规则（精细配置）：不能使用“ANY”等任意的、宽泛的策略，必须精细配置每一条通信需要开放的 IP、服务和端口，实现通信完全受控。

Negate rule,Used instead of the broad and permissive “any rules.” Negate rules provide tighter permission rights by specifying what system can be accessed and how.

5.网络地址转换(NAT)

防火墙可以改变每个外出流量的源地址(从可信不可信网络)到不同的地址。一个不可路由的地址（私网地址）是不会被互联网路由器转发的，因此，如果远程攻击使用不可路由的内部地址，是不能在开放的互联网上路由的。匿名是另一个使用 NAT 的理由。NAT 也极大地扩展了组织的 IP 地址空间能力，使 IPv4 地址可以继续使用。详细的 NAT 在 C.5 章节里讲。

6.端口地址转换(PAT)

以前叫动态 NAT。PAT 是 NAT 的延伸，是将所有内部地址的源端口号的映射到一个可路由 IP 地址的不同端口上去。使用了 PAT 的端口映射技术，将允许防火墙跟踪多个通信会话。

7.入侵检测和防御系统(IDS/IPS)

有两大类：

*基于主机的 IDS/IPS，监控服务器和工作站的活动

*基于网络的 IDS/IPS，监控网络活动。

入侵检测的探测有好几种。在第 7 域 H.2 章节详述。

8.安全事件管理(SEM)/安全事件和意外管理(SEIM)

SEM/SEIM 是一个解决方案，包括，从各种不同的来源、服务器或资产信息中收集日志和事件，并分析这个复杂情况，形成综合报告视图。同样，整个 IT 基础设施可以部署集中化的大范围的 SEM/SEIM 系统，对日志和事件信息进行集中管理。SEM/SEIM 不仅将综合日志将进行分析，根据既定怀疑模型，发现异常时还会发出警报。

B.4 端点安全（终端安全）

也就是终端安全。每个单独设备必须维护本地安全，不论其网络或通信通道是否提供安全。有时这被表示为“末端设备应对它自己的安全负责”。每个系统都应该有合适的安全组合，包含本地主机防火墙、反恶意软件扫描、身份验证、授权、审计和垃圾邮件过滤器以及 IDS/IPS 服务。还要打补丁，裁减服务什么的。等级防护评测最后肯定要检查终端的。

B.5 内容分发网络

内容分发网络 CDN（Content Distribution Networks），或叫内容转发网络，是一个资源服务的集合，其部署在互联网许多数据中心上以提供低延迟、高性能、高可用性和承载的内容。其实就是在各地的节点安装一个缓存服务器，提高并发访问效能。如今，CDN 服务是互联网内容的一个主要服务分支，包括 Web 对象(文本，图形和文字)，下载对象(可下载媒体文件，软件，文档)，应用(电子商务，门户网站)，流媒体直播，点播流媒体，社会网络。

B.6 物理设备

详见 B.1 章节。

C. 设计与建立安全通信信道

为特定应用通信信道提供安全服务协议被称为安全通信协议。先列一些主流的安全通信协议，重要的在后面再详细介绍：

1. 用于安全通信的（必考）

①IP 简单密钥管理(SKIP) Simple Key Management for Internet Protocol

这是一种用于保护无会话数据报协议的加密工具(无线 WAP 用了)。SKIP 被设计为与 IPSec 相结合，并且在 OSI 模型的第三层上工作。SKIP 能够对 TCP/IP 协议族的任何子协议进行加密。SKIP 在 1998 年被互联网密钥交换(IKE)替代。

②软件 IP 加密(swIPe) Software IP Encryption

这是另一种第三层 IP 安全协议。它通过使用封装协议来提供身份验证、完整性和机密性。

③安全远程过程调用(S-RPC) Secure Remote Procedure Call

这是一种身份验证服务，只是防止在远程系统上在未经授权的情况下执行代码的手段。

④安全套接层(SSL) Secure Sockets Layer

这是一种由 Netscape 开发的加密协议，目的是保护 Web 服务器和 Web 浏览器之间的通信。SSL 可以被用于保护 Web、电子邮件、FTP 甚至 Telnet 通信的安全。SSL 是一个面向会话的协议，使用对称密钥来加密数据，使用非对称密钥来进行对等认证（Peer Authentication），它提供了机密性和完整性。SSL 使用 40 位密钥或 128 位密钥进行部署。CISSP 认为 SSL 位于传输层（网络层之上，应用层之下），实际上它由两个协议组成：一个工作在会话层的底部，另一个工作在传输层的顶部。在 SSL 上运行的 HTTP 就是 HTTPS（HTTP Secure）。

POODLE 漏洞(Padding Oracle On Downloaded Legacy Encryption vulnerability)，可被攻击者用来窃取采用 SSL3.0 版加密通信过程中的内容，又被称为“贵宾犬攻击”。虽然该攻击利用有一定的难度，需要完全控制网络流量，但在公共 wifi 遍地都是和强调国家之间对抗的 APT 背景下，该漏洞仍有不小的影响。它迫使用户放弃 SSL，选用 TLS。

⑤传输层安全(TLS) Transport Layer Security

TLS 的功能类似于 SSL，相当于 SSL3.1 版本，但是它使用更健壮的认证和加密协议。

SSL 和 TLS 都有以下功能特性：

*支持在不安全的网络中提供安全的客户-服务器方式通信，并防止篡改、欺骗和窃听。

*支持单向认证。

*使用数字证书支持双向认证。

*通常实现为一个 TCP 包的初始载荷，允许它封装所有的更高层协议的有效载荷。

*可以应用在低层，如在第三层(网络层)作为一个 VPN。这被称为 OpenVPN。

此外，TLS 能用于加密 UDP 和会话初始协议(SIP)连接。SIP 是一个和 VoIP 有关联的协议。

⑤安全电子交易(SET) Secure Electronic Transaction

这是一种在互联网上进行交易传输时所使用的安全协议。SET 的基础是 RSA 加密以及数据加密标准(DES)。主要的信用卡公司都支持 SET，例如 Visa 和 MasterCard 。然而，SET 没有被互联网广泛接受：相反，SSL/TLS 加密的会话是安全电子商务的首选机制。

⑥安全外壳 SSH (Secure Shell)

安全外壳(SSH)在功能上类似于一种隧道机制，它为远程计算机提供终端式访问。SSH 是一种能够用于通过网络访问另一台计算机的程序。SSH 在易受攻击的通道(如 Intemet)上提供身份验证和安全传输。两台计算机会进行握手，并且(通过 Diffie-Hellman)交换会话密钥，这个会话密钥将在会话过程中加密和保护传送的数据。SSH 应当取代 Telnet、FTP、rlogin、rexec 或 rsh 使用，它们提供的功能与 SSH 的功能是一样的，但是安全程度要低得多。

⑦IPSec/Intemet 协议安全(Intemet Protocol Security, IPSec)

必考，详见第四域 C.3 章节。

2.用于身份验证的（必考）

①密码身份验证协议(PAP) Password Authentication Protocol

这是一种用于 PPP 的标准身份验证协议。PAP 以明文的形式传递用户名和密码，不提供任何形式的加密；只是简单地提供了一种从客户端向身份验证服务器传输登录凭证的手段。

②挑战握手身份验证协议(CHAP) Challenge Handshake Authentication Protocol

这是在 PPP 链接上使用的一种身份验证协议。CHAP 对用户名和密码进行加密。它通过使用不能重放的“挑战——响应”对话来执行身份验证操作。在建立的通信会话持续期间，CAHP 也会定期对远程系统重新进行身份验证，从而验证远程客户端的持久性身份。这个活动对用户是透明的。

③可扩展身份验证协议(EAP) Extensible Authentication Protocol

这是一个身份验证架构/框架，而不是一种实际的协议。EAP 允许自定义身份验证安全解决方案，例如支持智能卡、令牌和生物测定学。

上述三种身份验证协议最初用在拨号 PPP 连接上。现在，大量的远距离连接技术(包括宽带和 VPN) 都应用了这些协议与其他很多较新的身份验证协议和概念。

④EAP，PEAP 和 LEAP

受保护的可扩展认证协议(PEAP)Protected Extensible Authentication Protocol 封装在一个 TLS 隧道中。PEAP 优于 EAP 是因为 EAP 假设信道已经被保护，但是 PEAP 实施自己的

安全。PEAP 在802.11 无线连接上用于保障通信安全。PEAP可以采用无线协议接入WPA和WPA-2连接。PEAP 也优于思科专有的EAP ，即轻量级的EAP 协议Lightweight Extensible Authentication Protocol (LEAP)。LEAP是思科对不安全WEP的一个对策。LEAP支持频繁的再认证和WEP密钥的变化（WEB使用单个认证和一个静态密钥）。然而，LEAP可以被各种工具和技术进行破解，包括漏洞利用工具Asleap。

C.1 语音

常规的专用分支交换/专用小型交换机/用户级交换机(PBX) Normal private branch exchange或普通传统电话服务(POTS)plain old telephone service 或公共交换电话网络(PSTN) public switched telephone network的语音通信容易遭受截获、偷听、分机窃听和其他利用。

1.互联网语音协议(VoIP)

VoIP是一种将语音封装成IP数据包并支持音频电话通过TCP/IP 网络进行连接的技术。一些VoIP系统其本质上是纯明文形式的通信，这将容易被拦截和窃听。

*呼叫ID可以轻易的被伪造，从而执行语音钓鱼(VoIP phishing)攻击或在网络中进行语音垃圾邮件(SPIT)攻击Spam over Internet Telephony。

*呼叫管理系统和VoIP电话本身漏洞可能会受到DOS攻击。

*黑客可能会通过欺骗用户进行回拨的方式发动中间人(MitM)攻击。man-in-the-middle

*不加密的VoIP流量可以通过解码的方式被监听。

电信诈骗什么的社会工程学就不提了。

2.直接拨入系统访问控制DISA

PBX系统的“安全”一般会用直接拨入系统访问控制(DISA)，此系统被设计为通过为用户指派访问码来帮助管理PBX的外部访问和外部控制。

这种系统会遭到飞客（phreaker）的危害和滥用。一旦外部的飞客获悉了PBX访问码，他们往往能够完全控制和滥用公司的电话网络，这包括使用PBX将长途呼叫的计费指向公司的电话账户，而不是指向飞客的电话。飞客行为(phreaking)是一种针对电话系统的特定攻击类型。飞客使用各种技术回避电话系统，从而获得免费的长途呼叫、更改电话服务的功能、窃取特殊的服务甚至导致服务中断。下面列出了你需要了解的一些飞客工具（前提是已经搭线）：

①黑盒。控制线路电压，只是使用电池和线夹定做的电路板。（加电）

②红盒。模拟硬币存入付费电话时的声音来盗打电话，比如用磁带录音机。（投币）

③蓝盒。模拟与电话网络主干系统直接互动的2600Hz声音，可以是哨子、磁带录音机或数字音频生成器。（发声）

④白盒。用于控制电话系统，它是一种双音多频(DTMF)生成器(就是键盘)，维修员有这样的装备。（控制）

记忆：黑电（黑店）、红币（人民币）、蓝声（男声）、白控。

3.传真的安全

可以通过传真加密器、链路加密、活动日志以及异常报告提高安全性。

C.2 多媒体协作（例如：运程会议技术、即时消息）

视频会议，即时消息 IM，互联网中继聊天 IRC 什么的，它们有三种类型：

①P2P 网络；②代理通讯；③面向服务的网络。它们的安全很重要，重点讲下电子邮件。

电子邮件服务器通过使用简单邮件传输协议(SMTP) Simple Mail Transfer Protocol 接收来自客户端的消息，向其他服务器传送这些消息，并且将消息存放入用户基于服务器的收件箱。除了电子邮件服务器之外，这个基础架构还包括电子邮件客户端。客户端通过邮局协议版本 3 (POP3) Post Offi ce Protocol version 3 或互联网消息访问协议(IMAP) Internet Message Access Protocol 从基于服务器的收件箱中检索电子邮件。互联网兼容的所有电子邮件系统都依赖于 X.400 标准定位和处理邮件。

Sendmail 是 UNIX 系统中最常用的 SMTP 服务器，Exchange 是 Microsoft 系统中最常用的 SMTP 服务器，而 GroupWise 则是 Novell 系统中最常用的 SMTP 服务器。

1.安全多用途互联网邮件扩展(S/MIME) Secure Multipurpose Internet Mail Extensions

S/MIME 通过公钥加密和数字签名为电子邮件提供了身份验证和隐私保护。通过 X.509 数字证书能够提供身份验证，隐私则是通过使用公钥密码术标准(PKCS)加密提供的（使用 PKI）。使用 S/MIME 可以构成两种类型的邮件：

①签名的邮件 signed messages：提供了完整性和对发送者的身份验证。

②安全封装的邮件 enveloped message：提供了完整性、对发送者的身份验证以及机密性。

MIME 对象安全服务 MIME Object Security Services (MOSS)为邮件提供身份验证、机密性、完整性和不可否认性。MOSS 利用了 MD2 和 MD5（Message Digest）算法、RSA 公钥以及数据加密标准(DES)，从而提供了身份验证和加密服务。经 MIME 加密的邮件格式后缀名为.P7S。

2.隐私增强邮件(PEM) Privacy Enhanced Mail

隐私增强邮件 PEM 是一种电子邮件加密机制，它使用 RSA、DES 和 X.509 提供了身份验证、完整性、机密性和不可否认性。

3.域名密钥识别邮件(DKIM) DomainKeys Identified Mail

DKIM 是一个重要的手段，通过域名的身份验证来检测邮件发送自哪个组织。

4.可靠加密/良好的隐私(PGP) Pretty Good Privacy

可靠加密/良好的隐私(PGP) 是一个使用多种加密算法对文件和电子邮件进行加密的公-私密钥系统。它使用 RSA 来管理密钥，使用国际数据加密算法(IEDA)来加密数据，使用 MD5 来提供完整性，使用公钥证书来提供身份验证，对消息进行加密签名来实现不可否认性，但是以后的版本提供了算法选择。PGP 不是标准，而是一个自主开发的产品。它获得互联网草根阶层广泛的支持。PGP 最初是任何人都可以使用的免费产品，但是随后又被分为两个不同的产品。PGP 是一种商业产品；而 OpenPGP 是一个正在开发的标准，GnuPG 依从这个标准，并且这个标准被免费软件基金会独立开发。

PGP 使用自己的数字证书，不使用 PKI 的 CA。也就是说，PGP 是端到端的互相信任，PKI 只信任 CA。PGP 的每个用户都有一个称为密钥环(key ring)的文件，它是从其他用户那里接收的公钥的集合。密钥环上的每个密钥都有一个参数，该参数表明相应用户的可信程度以及这个特定密钥的有效性。

C.3 远程访问（例如：VPN、屏幕截取、虚拟应用/桌面、远程办公）

这里讲远程接入的安全。客户端可以采用这样的形式建立远程通信会话：

①使用调制解调器直接拨号登录远程访问服务器。

②在互联网上通过 VPN 连接至某个网络。

③通过瘦客户端(thin-client)连接与某个终端服务器系统相连接。

当然，还有卫星什么的接入手段。

1.安全措施

①传输保护

各种加密，这可能包括 VPN、SSL，TLS、SecureShell (SSH)、IPSec 以及 L2TP。

②身份验证

可能包括密码验证协议(PAP)、挑战握手验证协议(CHAP)、扩展验证协议(EAP 或者它扩展的 PEAP 或 LEAP)、远程验证拨号用户服务(RADIUS) 以及终端访问控制器访问控制系统(TACACS+)。

一个集成的身份验证机制通常使用 802.1x，即 EAP+RADIUS。

2.拨号协议

拨号协议的两个最主要的例子，PPP 和 SLIP。

①点对点协议(PPP) Point-to-Point Protocol

一种全双工协议，用于在各种非 LAN（局域网）连接上传输 TCP/IP 数据包，这些连接包括调制解调器、ISDN、VPN 和帧中继等。它通过使用各种协议(例如 CHAP 或 PAP)实现身份验证。PPP 是替换 SLIP 的协议，并且可以支持任何 LAN 协议，而不是只支持 TCP/IP。

②网络串行线路协议(SLIP) Serial Line Internet Protocol

这是一种较老的技术，用于支持异步串行连接(例如串行线缆或调制解调器拨号)上的 TCP/IP 通信。SLIP 已很少使用，不过仍然得到很多系统的支持。SLIP 只能够支持 IP 协议，需要静态的 IP 地址，不提供差错检测或纠正功能，并且不支持压缩。

3.集中化的远程身份验证服务

集中化的远程身份验证服务(例如 RADIUS 和 TACACS+) 就提供了这种额外的保护层。具体看第五域 B.3 章节吧。

4.远程访问服务

这里描述的服务许多用于 UNIX 操作系统。

①Remote Shell (RSH)

从概念上讲，因为它们是建立在相互信任的基础上，因此可以滥用于被获得水平访问权限和垂直提升权限的攻击。它们的认证和传输能力在设计时没有考虑安全性，因此，它们必须使用封装(如，X11)或通过 SSH 代替 Telnet 和 Rlogin，来获得安全性。

②Telnet

是一个基于命令行的协议，其设计目的是给通过命令行访问到另一个主机。虽然 WINDOWS 实现了这个协议，但 telnet 的最初是用在 UNIX 服务器世界中，事实上，一个 telnet 服务器是任何 UNIX 服务器标准配置。它存在的问题：

*极不安全，事实上，它使用在不受信任的环境中，会造成严重的安全隐患。

*提供有限的用户名/密码认证。

*不提供加密。

一旦攻击者获得了正常用户的凭据，他很容易完成权限升级，他可以在机器上传输数据和执行命令。作为运行在系统特权上的 Telnet 服务器，它本身就是一个有吸引力的攻击目标；攻击正使用 Telnet 服务器的漏洞可以提升系统权限。因此，建议安全从业人员在互联网和互联网连接的主机上停止使用 Telnet。事实上，标准的 Internet 服务器安全加固过程中，任何服务器都应该禁用的 Telnet 服务，在 UNIX 系统通常运行 telnet 进程下，并应利用 ssh v2 远程管理和管理所需的范围。

③远程登录(rlogin)，远程 shell(RSH)，远程复制(RCP)

rlogin 是一种使用 rlogin 授予远程访问机器的协议，通常是一个 UNIX 服务器。

同样，RSH 被赋权直接远程命令执行，RCP 拷贝数据或远程机器。如果一个 rlogin daemon (rlogind)进程，在一台主机上运行远程访问，可以通过两种方式获得：

*通过中央配置文件使用；

*通过用户配置。

后者，用户可以授权访问，而不是由系统管理员允许的。同样的机制适用于 RSH 和 RCP，虽然他们都是依靠不同的守护进程(rshd)。其认证是基于主机/IP 地址，虽然基于用户 ID 的 rlogin 授予访问权限，但它不做验证：即，如果请求来自受信任的主机，则 ID 远程客户端所声明的权限，即被授予给该 ID，rlogin 协议传输数据没有加密，因此受窃听和截取。

更安全的 SSH v2，可以替代 rlogin,rsh 和 rcp。

④SSH

相当于 SSL+Telenet

SSH 隧道的保护通信的完整性，防止会话劫持，中间人攻击。有两个不兼容的版本，SSH-1 和 SSH-2。SSH-2 具有改进的完整性检查(SSH-1 容易由于弱 CRC-32 完整性检查插入攻击)，支持本地扩展和数字证书等类型，如，开放 PGP 的。SSH 的最初设计是为 UNIX，但现在的操作系统都支持 SSH，包括 Windows, Macintosh 的实现，和 OpenVMS。

5.永久虚拟电路(PVC)和交换虚拟电路(SVC)

虚电路为终端系统连接提供高带宽、多用户电缆或光纤的一个专用的物理电路，其表现为一个专有电路。有两种类型的虚电路，基于当电路中的路径建立。

*在永久虚电路 PVC 中，当电路被购买后，运营商配置电路的路线。除非承运人改变路线调整网络，或响应一个中断等，否则路线不会被改变。

*另一方面，一个交换虚电路 SVC 用于动态配置，更像是一个拨号连接。

5.虚拟私有网络（VPN）Virtual Private Network

VPN 是上一章的内容，和 IPsec、SSL 一起放到本章来讲。这个是**必考**的。

虚拟专用网(VPN)是一个通信隧道，它可以在不可信的中间网络上提供身份验证和数据通信的点对点传输。大多数 VPN 使用加密技术来保护封装的通信数据。VPN 在不安全的或不可信的中间网络上提供了机密性和完整性，但是并不提供和保证可用性。

①隧道技术

你能真正理解 VPN 之前，你必须先理解隧道技术。隧道技术是网络的通信过程，它通过将协议包封装到其他协议包中来保护协议包的内容。隧道技术可以用在很多场合(如绕过防火墙、网关、代理或其他通信控制设备时)。通过将受限制的内容封装入已授权传输的数据包，就可以实现旁路。每当使用安全的 SSL 或 TLS 访问 Web 站点时，就会使用到隧道技术，此时明文 Web 通信通过隧道技术被装入 SSL 或 TLS 会话。此外，如果使用互联网电话或 VoIP 系统，那么语音通信会通过隧道技术被装入某种 VoIP 协议。

隧道技术也存在缺点：隧道会消耗额外的网络带宽。此外，隧道技术是一种点对点的通信机制，并且设计时没有考虑对广播通信的处理。隧道技术也使得在某些情况下监控流量的内容变得很难。

②VPN 协议

有四种常用的 VPN 协议：PPTP, L2F, L2TP 和 IPSec。（SSL/TLS 也可以被用来作为一个 VPN 协议，而不只是作为一个工作在 TCP 之上的会话加密。不过 CISSP 并不把 SSL/TLS 作为 VPN 来考。）

PPTP+L2F=>L2TP；L2TP+IPSec=VPN。

PPTP, L2F, L2TP 工作在第二层，IPSec 在第三层；

PPTP, L2F,IPSec 仅用于 IP 网络，L2TP 可用于任何局域网协议（LAN）。

VPN 总结如下表，协议详述在后面：

VPN 协议	自带身份验证保护?	自带数据加密?	支持的协议	支持拨号链接?	同时存在的连接数
PPTP	是	否	只支持 IP	是	单个点对点连接
L2F	是	否	只支持 IP	是	单个点对点连接
L2TP	是	否(可以使用 IPSec)	支持任何协议	是	单个点对点连接
IPSec	是	是	只支持 IP	否	多个连接

1.点对点隧道协议 Point-to-Point Tunneling Protocol

点对点隧道协议(PPTP)是从拨号协议点对点协议(PPP)开发出来的一种封装协议。它工作在 OSI 模型的数据链路层(第二层)，依靠通用路由封装(GRE)来建立隧道，并且被用在 IP 网络中，PPTP 不支持 TACACS+和 RADIUS。PPTP 在两个系统之间创建了一个点对点隧道，并且封装了 ppp 包。使用与 PPP 相同的身份验证协议，这些身份验证协议包括：

①Microsoft 挑战握手身份验证协议(MS-CHAP)

②挑战握手身份验证协议(CHAP)

③密码身份验证协议(PAP)

④扩展身份验证协议(EAP)

⑤Shiva 密码身份验证协议(SPAP)

CISSP 考试的重点是 PPTP 的 RFC2637 版本，而不是微软版本的实现，那个版本进行了专有修改并使用微软点对点加密（MPPE）来支持数据加密。PPTP 使用的最初隧道协商过程并没有加密。因此，包含发送者和接收者 IP 地址(可以包括用户名和散列密码)的会话建立通信包可能被第三方截获。PPTP 被用在 VPN 上，但是它常常被第二层隧道协议(L2TP)替代。L2TP 可

以使用 IPSec 为 VPN 提供通信加密。

2.二层转发协议 L2F 和二层隧道协议 L2TP/Layer 2 Forwarding Protocol and Layer 2 Tunneling Protocol

Cisco 公司开发了自己的 VPN 协议：第二层转发协议(L2F)，这是一种相互的身份验证隧道机制。然而，L2F 并不提供加密。L2F 没有得到广泛部署，并且很快被 L2TP 所取代。正如它们的名字所提示的，它们都工作在第二层。它们都可以封装任何局域网协议。

二层隧道协议(L2TP)源自于 PPTP 和 L2F 的组合。L2TP 会在通信的端点之间建立了一个点对点的隧道。L2TP 缺乏内置的加密方案，而是通常依赖 IPSec 作为它的安全机制。L2TP 还支持 TACACS+和 RADIUS。IPSec 通常为 L2TP 用做一种安全机制。

3. IP 安全协议/ IPSec/IP Security Protocol（重点）

目前最常用的 VPN 协议是 IPSec。IPSec 既是一个独立的 VPN 协议，又是用于 L2TP 的安全机制，并且只能用于 IP 通信。IPSec 提供了安全的身份验证以及加密的数据传输。IPSec 会改变数据包的报头中的 IP 地址，这可以被认为是一种攻击，因此，NAT 与 IPSec 不能同时工作。为了解决这两个协议的不兼容问题，可以使用 NAT 穿越(又名 IPSec NAT-T)技术，封装 UDP 端口 4500(参见 RFC 3948)。第三域 I.6 章节也提了下 IPSec。

IPSec 具有下列 3 个主要的组件或功能：

①身份验证头(AH)。AH 提供身份验证、完整性以及不可否认性。在每个数据包(头+数据)传输之前，一个使用共享秘钥加密数据包内容的哈希值(除了数据包路由时需要使用的信息，这个地址信息有可能改变)将被插入到 AH 包头中。终端系统之间协商使用哈希算法和共享密钥后，它们建立安全关联 SA。为帮助防止重放攻击(一个合法会话，被重新转发以获得未经授权的访问权限)，每个数据包在发送时，其 SA 都有一个序列号，并将其存储在 AH 中。在传输模式，AH 之间插入数据包的 IP 和 TCP 报头。AH 有助于确保真实性和完整性，不保证其机密性。加密是通过封装安全载荷(ESP)来实现的。

②封装安全有效载荷(ESP)。ESP 提供了加密，从而能够保护传输数据的机密性，也可以执行有限的身份验证操作。ESP 在网络层(第三层)上工作，包含四个部分：

*ESP 头部/报头：包含安全关联(SA)使用，数据包的序列号。和 AH 一样，ESP 给每一个数据包编一个序列号，以阻止重放攻击。

*ESP 有效负载：负载包含数据包的加密部分。ESP 通常使用对称加密算法。

*ESP 尾部：包括填充(填充字节)，满足要求的加密算法的分组字串长度。

*ESP 认证部分/身份认证：如果要使用身份认证，此 ESP 数据包字段应包含完整性检查值(Hash)。就像也相当于 AH 包头，终端系统相互协商身份认证算法来建立安全关联 SA。

ESP 有两种模式：

传输模式：只加密 IP 数据包，数据包的头部并没有进行加密。主要用于客户端和服务器等端到端的保护。

隧道模式：整个 IP 数据包都加密，并且新的数据包头被添加至 IP 数据包，从而能够控制通过隧道进行的传输。通常用于网络之间，如防火墙的 VPN。

③安全关联/安全联盟(SA)

SA 是终端系统间通信的沟通机制。所有的 SA 只能单向传输，双工通信必须要 2 个 SA。

④因特网密钥交换协议 IKE protocol

因特网密钥交换协议（IKE）允许两个设备“交换”对称密钥，用于在 AH 和 ESP 加密信息。有两种方式来“交换”密钥：

1 使用 Diffie-Hellman (DH) 式的协商

2.使用公钥证书（PKI）。IKE 会考到，但书上没写详细，算了。

4.SSL/TLS VPNs

SSL(安全套接字层)v3 和 TLS(传输层安全)v1.2 基本上是完全兼容的，最初的 SSL 加密工具是由 Netscape 开发，TLS 1.2 是由开放标准的 IETF 基于 SSL3.0 开发的。SSL 和 TSL 使用公钥证书进行彼此身份验证，它们相互认证。

SSL VPN 是远程访问的另一种方法。不像建立一个网络层的 IPSec VPN，SSL VPN 利用 SSL/TLS 创建隧道回到家庭办公室。远程用户使用 Web 浏览器来访问该组织的网络应用。即使用户使用 Web 浏览器，SSL VPN 不仅限于使用 HTTP。指插件的帮助下，如 Java，用户可以访问后端数据库，和其它非 Web 应用程序。SSL VPN 与 IPSec VPN 相比有几个优势。它们比 IPSec 更容易部署在客户端工作站,因为它们只需要一个 Web 浏览器,和几乎所有的网络允许传出 HTTP。SSL VPN 可以通过代理服务器的操作。此外，应用程序可以根据安全标准限制用户的访问权限，如外网网络用户，SSL 有助于建立企业的外联网络。

5.高保证互联网协议加密(HAIPE)

基于 IPSec 的 HAIPE 具有额外的限制和增强：例如，使用高保证硬件加密所有的通讯设备上对组播数据加密的能力，但是所有设备上的相同的密钥需要手工加载。HAIPE 是 IPSec 的一个扩展，可用于高度安全的通信，如，使用在军事应用。

高保障 IP 加密机 HAIPE：不通过网络来协商密钥，全部预置在硬件设备里，这样更安全。

C.4 数据通信（例如：VLAN,TLS/SSL）

1.网络拓扑 Network Topologies

环型 ring、总线型 bus、星型 star 和网状型 mesh。都很简单，不讲了。

2.单播 unicast、组播 multicast、广播 broadcast 还有任播 anycast

一对一的主机传输称为单播传输。

广播有特定的使用用途。已知一个路由器的 IP 地址，但不清楚设备的 MAC 地址时，路由器将广播地址解析协议(ARP)的请求，以解析设备的 MAC 地址。

多播就是组播，目的是要提供一个流，只传送感兴趣的主机。无线电广播是一种多播典型类型。选择一个特定的电台节目，你需要调整收音机的特定广播电台。同样，获得所需的多播服务，你需要加入相应的组播组。组播代理用于在网络及管理组播组中路由组播流量。每个支持组播的网络和子网络必须至少有一个组播代理。主机使用 Internet 组管理协议(IGMP)通告本地的组播代理，它想加入一个特定的组播组。组播代理也路由组播到本地主机的组播组成员和中继组播到邻近的代理。当一个主机要离开一个多播组，它发送一个 IGMP 消息到本地组播代理。组播不使用可靠会话。因此，组播是尽力而为的传送，不保证数据报接收。

任播允许源节点向一组目标节点中的任一节点发送数据报；在 DNS 防护中得到普遍引用。

3.交换网络

两个系统(单独的计算机或 LAN)通过多个中间网络连接肘，从一个系统向另一个系统传输数据包的任务是非常复杂的过程。为了简化这个任务，交换技术应运而生。

①电路交换网络（模拟）

主要用于电话网，PSTN 什么的。在终端系统之间，电路交换网络建立专用电路。这些电路由专用交换机连接。直到电路完全建立，终端系统开始通讯。终端系统使用专用电路及带宽。运营商计费是基于打开连接的持续时间电路的成本，这使得这种类型的网络终端系统间是稳定的经济通信。实例，电路交换网络是普通旧式电话服务(POTS)，综合业务数字网(ISDN)，和点对点协议(PPP)。

②分组交换网络（数字）

端系统之间的分组交换网络不使用专用连接。相反，数据分割分为数据包在一个共享的网络传输。每个数据包中包含的元信息，它可以独立地在网络中路由。网络设备将尝试为每个数据包目的地寻找最佳路径，数据包可以采取不同的路径和不同的顺利到达网络对端。目标端点有责任确保接收到的数据包，以正确的顺序在堆栈中重组。

4.虚拟局域网 Virtual LAN

虚拟局域网（VLAN）被用于硬件上以实施网络分割，这是交换机的最基础功能。搞网络的都配过 VLAN，没什么好说的。

VLAN 可以控制流量，管理子网，对安全而言有以下功能和好处：

①控制和限制广播流量。阻断在子网和 VLAN 中的广播。

②在子网之间隔离通信和流量。

③减少网络被监听的脆弱点。

④抑制对抗广播风暴(泛洪攻击)。

⑤端口隔离或私有端口。

5.广域网 WAN

搞通信的，做主干网维护的就很清楚。一般分为专线（电信信道）和非专线（拨号）。

专线有欧洲标准和美国标准，都是基于电信光纤传送网的传输系统。

①美国电信专线

0 级数字信号 DS-0，T1，64K 到 1.544M；

1 级数字信号 DS-1，T1，1.544M，24 路电话；

2 级数字信号 DS-2，T2：4×T1，6.312M；

3 级数字信号 DS-3，T3：7×T2，28 个 T1，44.736M；

4 级数字信号 DS-4，T4：6×T3，274.176M。

②欧洲电信专线（中国用的多）

欧洲数字传输格式 1，E1：2.048M；

欧洲数字传输格式 2，E2：8.848M； E3：34.304M； E4：139.264M。

Optical Carrier (OC) Bandwidth：

OC-1：51.84M； OC-3：155.52M

OC-9：466.56M； OC-12：622.08M

OC-18：933.12M；　　OC-24：1244.16M

OC-36：1866.24M；　　OC-48：2488.32M

OC-192：9953.28M。

③数字用户线路(DSL)

DSL 技术利用升级电话网使用户的通信速度达到 144Kbps 至 6Mbps(或更高)的水平。DSL 存在多种格式，例如 ADSL、xDSL、CDSL、HDSL、SDSL、RASDSL、IDSL 与 VDSL，每种格式的区别在于所提供的下行带宽和上行带宽有所变化，最大传输距离大有几公里。针对考试而言，只需要理解 DSL 的总体概念。

*不对称数字用户线(ADSL)：下行传输速率比上行的大得多，一般是 256 到 512 Kbps 的下游和上游 64 kbps。

*速率自适应 DSL(RADSL)：上行传输速率自动调整基于线路质量。

*对称数字用户线(SDSL)：使用相同的速率上行和下行传输。

*高速 DSL (VDSL)：支持的传输速率比其他 DSL 技术更高，如 13Mbps 下行和 2Mps 上行。

*宽带 DSL(HDSL) High-Data-Rate Digital Subscriber Line：上下行相，都是 1.544Mbps。

④综合业务数字网(ISDN)

ISDN 是一种完全数字化的电话网，能够同时支持语音通信和高速数据通信。ISDN 服务格式存在两种标准等级或格式：

基本速率接口(BRI)。为客户提供的连接具有两个 B 信道和一个 D 信道。B 信道支持 64Kbps 的吞吐量，被用于数据传输。D 信道则用于电话，带宽为 16Kbps。尽管没有设计 D 信道支持数据传输，BRI 仍然号称为客户提供的总吞吐量为 144Kbps。（运营商坑爹）

主速率接口(PRI)。为客户提供的连接具有 2 至 23 个 64Kbps 的 B 信道和一个 64Kbps 的 D 信道。因此，我们部署的 PRI 最小为 192Kbps，最大为 1.544Mbps。不过需要记住的是，因为包含不能用于实际数据传输的 D 信道，所以这些数字指的是带宽而不是数据吞吐量。

还有卫星什么的，不考。

⑤其它各种广域网连接技术（都是分组交换）

WAN 为 LAN 提供了入网的所有接口。边界连接设备称为信道服务单元/数据服务单元(CSU/DSU)。这些设备将 LAN 信号转换为网络运营商网络所使用的格式，反之亦然。CSU/DSU 包含数据终端设备/数据电路终端设备(DTE/DCE)，这些设备为 LAN 的路由器(DTE)与 WAN 运营商网络的交换机(DCE)提供了实际的连接点。CSU/DSU 起到了转换器、存储转发设备与链路调节器的作用。CSU/DSU 存在多种类型，如 X.25、帧中继(Frame Relay)、SMDS 与 ATM。

channel serviceunit/data service unit (CSU/DSU),

data terminal equipment/data ircuit-terminating equipment (DTE/DCE),

在单位负责十几年网络的人应该经历了主干网技术的演变。

X.25 连接

X.25 是一种出现较早的分组交换技术，并且在欧洲范围内被广泛应用。这种技术使用永久虚电路在两个系统或网络之间建立特定的点对点连接。X.25 是帧中继的前身，二者的运作方式几乎一模一样。不过，与帧中继或 ATM 相比，X.25 自身的性能较低、吞吐速率较慢，因此在逐步走向衰落。

帧中继连接 Frame Relay

与 X.25 一样，帧中继也是一种使用 PVCs（永久虚电路）的分组交换技术，工作在第二层。然而与 X.25 不一样的是，帧中继连接支持**多条 PVC**s。帧中继是一种使用分组交换技术在通信终端之间建立虚电路的第二层连接机制。专线或租用线的成本主要取决于通信终端之间的距离，而帧中继的成本主要取决于传输的数据量。帧中继网络是一种共享介质，提供点对点通信的虚电路就被创建在这种介质中。所有虚电路都是独立的，并且彼此不可视。

承诺信息速率(CIR) committed information rate 是一个与帧中继相关的重要概念。CIR 是服务提供商向其客户保证的最小带宽，通常远小于服务提供商网络的实际最大带宽。

帧中继要求在每个连接点上都使用 DTE/DCE。客户拥有 DTE (类似于路由器或交接机，并且为客户的网络提供对帧中继网络的访问)。帧中继服务提供商拥有 DCE，从而完成数据在帧中继网络中的实际传输以及为客户建立和维护虚电路。T 是 terminal，C 是 central，很好理解吧。

SMDS

交换式多兆位数据服务(SMDS) Switched Multimegabit Data Service 是一种无连接的分组交换技术。通常，SMDS 用于连接多个 LAN，从而组成一个城域网(MAN)或 WAN。如果需要链接极少通信的远程 LAN，那么 SMDS 往往是首选的连接机制。SMDS 支持高速的突发通信量，并且支持按需分配带宽。SMDS 机制将数据分片为若干小的传输信元。考虑到使用了相似的技术，所以可以将 SMDS 视为 ATM 的前身。

ATM

异步传输模式(ATM) Asynchronous transfer mode 是一种信元交换 WAN 通信技术。这种技术将通信分片为若干长度固定为 53 字节的信元。通过使用长度固定的信元，ATM 更有效率，并且能够提供更高的吞吐量。ATM 既可以使用 PVC ，也可以使用 SVC。ATM 提供商保证其租用服务的最小带宽与指定的质量等级。ATM 是一种面向连接的分组交换技术。

⑥专门的广域网协议

某些 WAN 连接技术需要使用其他专门的协议来支持各种各样特殊的系统或设备。主干路由器上经常会看到。如：

同步数据链路控制(SDLC) Synchronous Data Link Control

同步数据链路控制被使用在专门租用线路的永久物理连接上，从而为大型机(如 IBM 系统网络体系结构[SNA]系统)提供连通性。运作在 OSI 模型第二层(即数据链路层)的 SDLC 使用了轮询技术，是一种面向比特的同步协议。

高级数据链路控制(HDLC) High-Level Data Link Control

高级数据链路控制是 SDLC 的改进形式.专门针对同步串行连接而设计。HDLC 支持全双工通信，并且支持点对点连接与多点连接。与 SDLC 一样，HDLC 使用了轮询技术，同样运作在 OSI 模型的第二层(即数据链路层)。此外，HDLC 还提供流控制，并且包括差错检测与校正。

高速串行接口(HSSI) High Speed Serial Interface

高速串行接口是一个 DTE/DCE 接口标准，它定义了复用器和路由器如何连接高速网络运营商服务(如 ATM 或帧中继)。复用器是一种能够实现在单条线路或虚电路上传输多种通信或信号的设备。HSSI 定义了接口或连接点的电气与物理特征，因此该协议运作在 OSI 模型的第一

层(即物理层)。

⑦拨号封装协议 Dial-Up Encapsulation Protocols

点对点协议(PPP)是一种封装协议，它被设计用于支持在拨号或点对点链接上传输 IP 通信数据。PPP 允许通过 WAN 设备的多供应商互用性来支持串行连接。所有拨号连接与大多数点对点连接性质上都属于串行连接(与并行连接相对)。PPP 包含众多通信服务，这些通信服务包括 IP 地址的分配与管理、同步通信的管理、标准化封装、复用、链接配置、链接质量测试、差错检测以及特性或选项协商(例如对压缩的协商)。

PPP 最初被设计用于支持针对身份验证的 CHAP 和 PAP 协议。不过，最新版本的 PPP 也支持 MS-CHAP、EAP 以及 SPAP 协议。此外，PPP 还可以用于支持网际包交换协议(IPX) 和 DECnet 协议。PPP 在 RFC1661 文档中记录为互联网标准。PPP 替代了串行线路互联网协议(SLIP)。SLIP 只支持半双工通信，没有提供身份验证，不存在差错检测能力，并且要求人工建立与关闭链路。

6.安全边界

安全边界是任何两个具有不同安全要求或需求的区域、子网或环境之间的交线。安全边界存在于高安全性区域和低安全性区域之间，例如某个 LAN 和互联网之间。识别你的网络上和现实世界中的安全边界十分重要。一旦你确定了安全边界，那么你就需要部署某些控制和机制，从而控制跨越这些安全边界的信息流。

7.简单网络管理协议(SNMP)

SNMP 是设计用来管理网络基础设施。SNMP 包括管理服务器客户端，客户端安装在网络设备，如路由器和交换机，也被称为代理人。SNMP 允许管理端“GET”的代理变量的值，以及“SET”赋值变量。

最容易利用 SNMP 的漏洞是一个蛮力攻击，用来猜测容易的密码，这个密码被称为“SNMP 团体字符串”，常常用来管理远程设备。社区字符串是一个潜在的严重风险，但也是容易减轻的风险。直到 V2 版本，SNMP 没有提供任何程度的身份认证和传输的安全性保护。身份认证只包括一个叫做社区字符串的标识符，由管理端自己确认，并使用特定的密码对代理(这个字符串被配置成代理)发送命令。在这种情况下，密码很容易被截获，从而导致命令被嗅和可能的伪造。SNMP 版本 2 不支持任何形式的加密，使用明文形式的密码(社区字符串)。SNMP 版本 3 针对这一弱点，使用了加密的密码。

C.5 虚拟化网络（例如：SDN、虚拟 SAN、来宾操作系统、端口隔离）

VMware 已经用的很多了，比较好理解。虚拟软件也没什么好说的。

1.虚拟桌面 virtual desktop

这个术语指的是至少三种不同类型的技术：

①远程访问工具。授予用户访问一个远程的计算机系统，允许远程查看和远程桌面的显示、控制键盘、鼠标等。

②扩展的虚拟应用。封装多个应用和某种跨操作系统的桌面形式，给用户提供了一个综合平台而无需多台电脑。

③扩展或扩展桌面。使用户可使用多个应用程序的布局，使用按键或鼠标动作之间的切换。

2.虚拟网络 Virtual Networking

虚拟化网络或网络虚拟化是将硬件和软件版网络组件组合成一个单一的集成实体。由此产生的系统允许软件控制所有网络功能：包括管理，流量整形，地址分配等。虚拟化网络就是软件定义网络 SDN，当然也包括虚拟 SAN 等。

软件定义网络 SDN 也是虚拟网络，在 A.5 章节里讲清楚了。

3.软件定义的存储和虚拟 SAN

虚拟 SAN（存储区域网络)也是一个网络技术，它将多个单独的存储设备组合成一个单一的综合网络访问存储容器。一个虚拟 SAN 或软件定义的共享存储系统是一个在虚拟网络或 SDN 上虚拟的 SDN。

软件定义存储(SDS)的一个基本前提是管理程序(存储中的操作系统)是数据中心新的裸机部署在一个软件定义的数据中心(SDDC)，所有的服务都是建立在虚拟化层，它不仅明确分离出数据平面和控制平面，但也允许存储功能延伸到生成时间。不是依靠严格的硬件构建满足所有工作负载的需求，特性和政策可以通过虚拟机管理程序。管理程序和 SDS 一起通过提供 API 菜单服务，来了解各种硬件设备的功能和使用正确的功能和性能的需要，在每一个虚拟机的基础上。在 SDS，硬件是增强软件功能强大的机制，使所有的 X86 节点参与扩展、分布式集群，可以用线性的方式扩展规模，而没有太多的整体限制。在这种规模的存储模型，每一个 x86 节点包含直接连接硬盘和固态存储，可以通过所有节点和所有的工作负载来均衡影响。此外，规模化不仅适用于存储容量，而且适用于存储控制逻辑，有助于在规模扩张时，避免性能瓶颈。

作为与 SDN 案例，SDS 寻求分开的物理存储硬件和存储逻辑.存储逻辑决定数据放置和什么服务应用中的读写操作。这将导致存储层非常灵活，能够适应变化的应用需求。它还创建了一个统一的、一致的数据结构，每个虚拟机保持充分的可见性。

存储服务要提供：动态分层、缓存、复制、服务质量 QOS、快照、去重、压缩、克隆。

基于 SDS 存储系统提供保护和数据可用性机制的几种类型：

①智能数据布局：数据保护开始于第二份数据写入物理磁盘并确认应用负载。在 SDS 的存储系统,数据放置和保护是至关重要的,因为没有基于硬件的 RAID 数据保护工作机制。在 SDS ，数据布局可能发生若干次。

②控制器：SDS，基于软件的控制器负责确保数据从磁盘读写的可用性，保证数据可以被应用程序和虚拟机使用。软件控制器往往是冗余的，用于帮助环境保持高水平的可用性，即使在发生故障的时候。

③软件 RAID：通过 SDS，基于硬件的 RAID 系统不再使用，现在主要使用基于软件的 RAID，符合概念的 SDS ，这些 RAID 构建必须被基于软件的控制器完全支持，并且，必须能够扩展以满足企业级的容量和性能需求。

4.网络地址转换 NAT

NAT 是一种将包头中的内部 IP 地址转换为公共 IP 地址从而在互联网上进行传输的机制。NAT 只能被用在 IP 网络中，并且在 OSI 模型的网络层(第三层)上工作。

NAT 的功能和好处有：

①只租用少量的公网 IP 地址。

②局域网使用专用 IP 地址（私网 IP 地址）。

③隐藏内部 IP 地址方案和网络拓扑结构。

④通过限制连接提供了保护，只有来自于内部受保护网络的连接才被准许从互联网返回网络，减少 DOS 攻击。

通常，安全专家提到的 NAT 实际上是 PAT。端口地址转换(PAT)将一个内部的 IP 地址映射为一个外部 IP 地址和端口号的组合。因此，PAT 理论上在单个外部租用 IP 地址上可以支持 65536(2^{32})个来自内部客户端的、同时发生的通信。如果使用 NAT，那么租用的公共 IP 地址数必须与期望同时发生的通信数相同，不然内网还是出不去。

IPv4 的可用地址空间只有 40 亿个(2^{32})，早期设计者具有很好的前瞻性，他们为专用的无限制的网络留出了一些地址空间。这些 IP 地址通常被称为专用/私网 IP 地址,在 RFC1918 中进行了定义，如下所示：

*10.0.0.0~10.255.2S5.2S5（整个 A 类范围）

*172.16.0.0~172.31.255.255（16 个 B 类范围）

*192.168.0.0~192.168.255.25S（255 个 C 类范围）

你可以使用的 NAT 有两种模式：静态和动态。

静态 NAT

将特定的内部客户端的 IP 地址被永久地映射到特定的外部公共 IP 地址时，就会使用静态模式的 NAT，静态 NAT 也会允许外部实体与专用网络内部的系统进行通信。

动态 NAT

动态模式的 NAT 允许多个内部客户端使用较少的租用公共 IP 地址。因此，即使租用的公共 IP 地址较少，较大的内部网络仍然能够访问互联网。在动态模式的 NAT 中，NAT 系统维护了一个映射数据库，从而使来自互联网服务的所有响应信息正确地路由至最初的内部请求客户端。NAT 常常与代理服务器或代理防火墙相结合，从而提供额外的互联网访问和内容缓存功。

因为 NAT 更改了数据包头，而 IPSec 依赖数据包头来阻止安全违规，所以 NAT 并不直接与 IPSec 相容。不过，某些版本的 NAT 代理被设计为在 NAT 上支持 IPSec。

5.自动私有 IP 地址寻址 Automatic Private IP Addressing

一旦 DHCP 分配失败，自动私有 IP 地址寻址(APIPA)，又叫做本地链路地址分配会为系统指派 IP 地址。APIPA 基本上是一项 Windows 功能。APIPA 为每个失败的 DHCP 客户端指派从 169.254.0.1 到 169.254.255.254 范围内的一个 IP 地址(以及默认 B 类子网掩码 255.255.0.0)。这允许系统与同一广播域内其他配置 APIPA 的客户端进行通信，但是不能跨越路由器与任何系统通信，也不能与正确分配了 IP 地址的任何系统通信。

不要混淆 APIPA 和 RFC1918 定义的私有 IP 地址范围。APIPA 通常不直接涉及安全。然而，它仍然是一个需要重点理解的问题。如果你发现一个系统分配一个私有地址而不是有效的网络地址，这表明是一个问题。它可以是 DHCP 服务器的电缆或电源故障，但也可能是对 DHCP 服务器恶意的一个攻击征兆。你可能会被要求解释问题 IP 地址出自哪里。你应该能够判断一个地址是一个公共地址、一个 RFC1918 私有地址、一个 APIPA 地址，或一个环回地址。

169.254 的 IP 经常会遇到的，笔记本连接一个 CMCC 或 CHINANET 的共用 WIFI 点的时候，经常不成功就出现这个地址了。

6.网络存储

①独立磁盘冗余阵列(Redundant Array of Independent Disks, RAID)

为硬盘提供容错功能，并且能够改善系统性能。镜像(也称为 RAID 1)和双控过程中，每一个写入数据的操作都在几个物理位置同时或几乎同时发生，提供一定程度的容灾难能力。镜像和双控之间的区别在于：使用镜像时，写入数据的两个(或多个)物理位置需要依赖同一个控制器，因而存储仍然会受到控制器本身的单点失败影响；双控则使用两个或几个控制器。

RAID 经常考 1、5、6、10，在第七域 K.1 章节详述。

②直接访问存储设备(Direct Access Storage Device DASD)是磁性磁盘存储设备使用的一个常用术语；历史上，它曾用在大型机和小型计算机环境内。RAID 就是一种 DASD。

③大规模非活动磁盘阵列(Massive Array of Inactive Disks)， MAID 是一种最近才进入中型存储设备(数百兆兆位)市场的产品。由于很少访问的驱动器的电源被断开，因此能源消耗明显减少，磁盘驱动器的使用寿命也随之延长。较小的存储需求通常不适合于采用 MAID。至于需要大量写操作的最高端的存储需求，磁带驱动器仍然是最经济的解决方案。

D.预防和减缓网络攻击

网络攻击的类型、方法、技术很多很杂，在第九域有汇总，要自己慢慢梳理。

1.DoS 和 DDoS/ denial-of-service

拒绝服务攻击是一种资源消耗型攻击，它以阻止受害系统的合法活动为主要目标。DoS 不是一个单一的攻击，而是指一类攻击。一些攻击利用操作系统软件的缺陷，而其他的则把重点放在安装的应用程序、服务或协议。一些攻击利用具体的协议，包括互联网协议 IP，传输控制协议 TCP，lnternet 控制消息协议(ICMP)和用户数据报协议 UDP 等。

靠一台主机攻击显然力量不够，最好是 DDOS，通过僵尸网络来搞，还能隐藏自己。

怎么防 DOS 不说了，应该都想得到。考试中有使用 tarpit 来防御 DOS，类似于蜜罐，是一个模拟的有漏洞的服务组件，当遭受一些非法扫描等攻击时，它会让攻击者的自动扫描的工具软件出现响应失败或连接超时。

2.偷听/窃听 Eavesdropping

窃听需要搭线。由于使用的是被动攻击方式，因此检测偷听设备和软件通常较为困难。如果偷听或窃听从而更改通信数据或在其中添加数据，则属于主动攻击类型。Sniffers、NetWitness、T-Sight、Wireshark、Zed Attack Proxy (ZAP)等好多工具可以用。

保证在内部基础架构之外安全可靠地传输数据是极其重要的，就是要加密。

3.假冒/伪装 Impersonation/Masquerading

模仿或是伪装，是一种假装是某人或假装是某物并获得未经授权而访问系统的行为。这通常意味着认证证书被窃取或者遭受篡改并满足(即成功地绕过)认证机制。这不同于欺骗，实体提出了一个虚假的身份但没有任何证据(如错误地使用 IP 地址、MAC 地址、电子邮件地址、系统名称、域名等)。模仿往往可以通过捕获网络服务会话设置中的用户名和密码加以实现。

对付假冒攻击的解决方案包括：使用一次性填充和令牌身份验证系统，使用 Kerberos ，使用加密，从而增加从网络通信中提取身份验证凭证的难度。

4.重放攻击 Replay Attacks

重放攻击是假冒攻击的一种，它可以利用通过偷听捕获的网络通信进行攻击。重放攻击企

图通过对系统重放被捕获的通信来重建通信会话。你可以使用一次性身份验证机制和序列化会话身份标识来防范重放攻击。

5.修改攻击 Modification Attacks

能够更改被捕获的数据包，然后再将其放回到系统中。被修改的数据包被设计为能够避开改良的身份验证机制和会话排序的限制。针对修改重放攻击的对策包括数字签名验证和数据包校验和验证。

6.地址解析协议欺骗 Address Resolution Protocol Spoofing

ARP 用于通过轮询使用系统的 IP 地址来发现该系统的 MAC 地址。对付 ARP 攻击的手段包括：为关键系统定义静态的 ARP 映射，监控 ARP 缓存中的 MAC-TP 地址映射，或者使用 IDS 检查系统通信中的异常以及 ARP 通信中的变化。

7. DNS 投毒、欺骗和劫持 DNS Poisoning, Spoofing, and Hijacking

详细的不想讲了，在第三域的 E.1 章节讲了。

8. 超链接欺骗 Hyperlink Spoofing

与 ARP 相关联的另一种攻击是超链接欺骗。这种类似于 DNS 欺骗的攻击用于将通信重定向至欺诈系统或冒名系统，或者简单地将通信发送至预定目的地之外的任何地方。超链接欺骗既可以采用 DNS 欺骗的形式，也可以只是简单地在发送给客户端的文档的 HTML 代码中修改超链接 URL，因为大多数用户并不通过 DNS 验证 URL 中的域名，而是认定超链接是合法的并进行点击，所以超链接欺骗攻击往往都会成功。

网络钓鱼(phishing)是另一种经常使用超链接欺骗的攻击。网络钓鱼意味着诱骗他人上钩，从而获得信息。这种攻击可以采用很多形式，包括使用伪造的 URL。

9.泛洪 flooding attack

泛洪这个词一点都不好听，也不知道是谁在什么时候发明的，洪泛这个词是错的。泛洪就是泛滥的意思，也有教材说泛洪是交换机和网桥使用的一种数据流传递技术，将某个接口收到的数据流从该接口之外的所有接口发送出去。如果数据帧中的目的 MAC 地址不在 MAC 地址表中，就要向所有端口转发，请示回应。泛洪攻击有以下几种：

①SYN 泛洪。利用 TCP 的三次握手机制，有两种：PING 包泛洪就是向目的大量 PING，死亡之 PING；smurf 就是向网络发大量改了回应地址的 SYS 包，让主机（或僵尸网）都把响应包发送给目的机。

②DHCP 泛洪。

③ARP 泛洪。

④UDP 泛洪。

10.VLAN 攻击

下面给出针对 VLAN 在数据链路层的最常见的攻击：

①MAC 洪泛攻击：这是不典型的网络“攻击”，但会限制所有交换机和网桥的工作方式。如果交换机的 ARP 地址映射表已满，地址不再被学习，则流量将被永久进行(来源口)端口泛洪(portsflooding)。

②802.1Q 和交换链路间协议(ISL)标记攻击：标记攻击允许在一个 VLAN 中的用户获得未经授权的访问权限，来访问另一个 VLAN。例如，如果一个 Cisco 交换机端口被配置为动态中

继协议(DTP)收到了假 DTP 包，它可能成为一个中继端口，并接受另外一个 vlan 的流量。这通常被称为“VLAN 泄漏”。这可以通过设置关闭所有非 DTP 信任端口进行防范，也可以通过简单的配置指南或软件的升级来防范。

③双封装 802.1q/nested VLAN 攻击：在交换机内，VLAN 号码和识别信息是放置在一个特殊的扩展格式，允许转发路径保持端到端隔离 VLAN 不丢失任何信息。ISL 是 Cisco 专有技术，在某种意义上是一个紧凑的扩展报头。一个 VLAN，没有明确对一个 802.1Q 链路相关的任何标签。这个 VLAN 是隐式用于一个 802.1Q 端口收到的所有未标记的通信能力。这种能力是可取的，因为它允许 802.1Q 端口能够与旧的 802.3 端口直接发送和接收数据流量。当双封装 802.1 Q 包注入到网络设备的 VLAN 是一个 TRUNK 的 native VLAN 时，这些数据包的 VLAN 标识不能从端到端保存，这是因为 802.1Q TRUNK 总是通过剥离外层标签修改数据包。在外部标签去除后，内部标签只有数据包的 VLAN 标识符。区此，采用两个不同的标签双封装数据包，流量可以跨越 VLAN。

④ARP 攻击：不说了。ARP 中毒或 ARP 欺骗还有中间人攻击什么的。

⑤组播暴力攻击：这种攻击试图利用交换机的潜在漏洞，发起二层多播帧的风暴。正确的行为应该是限制源 VLAN 的通信流量，不当的行为会泄露帧到其他 VLAN。

⑥生成树攻击：另一种攻击，试图利用可能的交换机的弱点发起 STP 攻击。攻击需要在链路上，嗅探得到 STP 帧，得到端口上开启的 STP ID，然后，攻击者会发送 STP 的配置/拓扑变化确认 BPDU，宣布他是一个很低的优先级的新根桥。

⑦随机帧暴力攻击：这最后的攻击，可以有很多形式，但总的来说是蛮力攻击，随机变化的一个或几个数据包字段，而保留了源地址和目的地址，等常数信息。

第五域　身份与访问管理　（访问控制与身份管理）

Chapters 13,14 in OSG 7th

Chapters 3 in AIO 6th

A. 控制资产的物理与逻辑访问

本节涉及的要访问的资产包括信息、系统、设备、设施、人员等一切有价值的东西，所以考试大纲就按这些顺序列出了要点，但内容有点太离散了。后面的内容就是按访问控制的流程来写的：标识=>验证=>授权=>访问=>问责。

访问 Access 就是存在主体 Subject（访问者）与客体 Object（对象）之间的信息流。

一、访问控制的类型

1. 第一种分类（访问控制的 7 个主要类型）：

第一域 I.6 章节就讲了访问控制的 7 个主要类型，即安全控制功能的分类：

①管理（Directive）/指引：指令性、强制性的规定，如：安全策略需求或标准、张贴通告、疏散路线出口标志、监控、监督、工作任务过程。

②威慑（Deterrent）：旨在打击潜在的攻击者。吓唬人别搞坏事，如：策略、安全意识培训、锁、围墙、安全标识、保安、陷阱、安全摄像机。

③预防（Preventive）：旨在避免发生事件。阻止非法进入，如：围墙、锁、生物测定学、陷阱、灯光、警报系统、责任分离、工作轮换、数据分类、渗透测试、访问控制方法、加密、审计、使用安全摄像机或闭路电视(CCTV)、智能卡、回叫、安全策略、安全意识培训、反病毒软件、防火墙和入侵防御系统。

④补偿（Compensating）：提供可替代控制措施。增加访问控制措施，如：对 PII（个人信息）加密。

⑤检测（Detective）/监测：确认事件的活动和潜在的入侵者。发现非法进入，如：保安、移动探测器、记录和检查安全摄像机或闭路电视捕获的事件(CCTV) 、工作轮换、强制休假、审计跟踪、蜜罐或蜜网、IDS、违规报告、对用户的监管和检查、事故调查。

⑥纠正（Corrective）/矫正：事件发生后，修复部件或系统。发生非法访问后，将系统还原至正常的状态，如：终止恶意行为或重启系统、删除或隔离病毒。

⑦恢复（Recovery）：目的是使环境恢复正常运作。比纠正性控制更高级、更复杂，如：备份和还原、容错驱动系统、系统镜像、服务器群集、反病毒软件以及虚拟机影像。

很多安全措施是同时符合以上多种类型的，如果问 CCTV 是预防、还是威慑、还是检测？就要看题目中的场景了，它发挥的实际作用是什么就选最佳答案。

2. 第二种分类：

管理性 Administrative。依照组织的安全策略和其它规则或需求，定义的策略与过程，即管理控制，主要关注两个方面：人员与业务实践。例如：策略、过程、雇用准则、背景调查、数据分类、安全意识和培训效果、报告与回顾、人员控制以及测试等。

技术性 Logical/technical。作为硬件或软件机制用于提供对这些资源和系统的保护，例如：认证方式(例如密码、智能卡、生物测定学)、加密、受限接口、访问控制列表、协议、防火墙、路由器、入侵检测系统以及阈值级别等。

物理性 Physical。包括部署以预防、监控或检测设施内的系统或区域直接接触的物理机制。例如：保安、围墙、移动探测器、闭锁的门、密封窗、灯光、线缆保护、笔记本电脑锁、徽章、磁条卡、看门狗、摄像机、陷阱以及报警器等。

3.第三种分类：

其实就是不同的访问控制模型，详见 E 章节。

DAC(Directionary)：自主访控：自己管。

UDAC（Undirectionary）：非自主访控：有系统管理员管。

MAC(Mandatory)：强制访控：主客都有安全标签，必须严格管。

RBAC(Role-Base)：基于角色访控：动态职责分离：在会话中限制权限。

rule-BAC：基于规则访控：很多规则。

ABAC(Attribute- Base)基于属性的访控。

A.1 信息

没内容。

A.2 系统

没内容。

A.3 设备

没内容。

A.4 设施

没内容。

B.管理人员与设备的身份和验证

B.1 实施身份管理 （例如：SSO,LDAP）

一、基础知识

1.有三个重要概念之间的关系要搞清楚：

访问控制的流程当中最重要的三个步骤要素：身份要唯一，认证要有效，授权要控制。

①身份标识提供了唯一性（身份）。ID

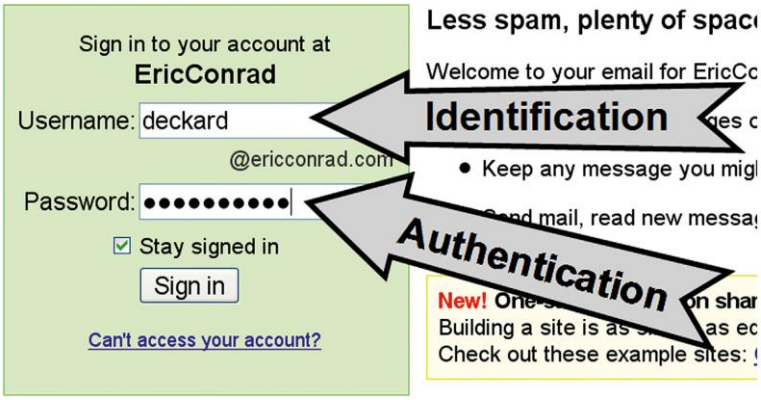
②认证（验证）提供了有效性。Authentication/IDentification

③授权提供了控制。Authorization

身份验证通常包含 2 个步骤：

①输入公共信息（用户名、ID 号）：身份标识步骤。

②输入私有信息（密码、PIN 码）：身份验证步骤。



创建和发布安全的合规的身份标识/帐户（ID），要满足 3 个关键条件或特性：

①唯一性。每个用户独一无二。

②非描述性。ID 不能透露隐私或敏感信息（比如用户的职位信息）。

③签发（安全发布）。ID 必须由权威机构签发和证明其真实有效。

2.有三个概念也要搞清楚：

这几个概念的考题很难。**权限=操作__许可=(访问+权限)__特权=超级许可**

*许可 Permissions。许可是指授予对一个对象的访问权并明确访问权的具体内容。有时与权限的意思一样。（许可包括能否访问客体、对客体有什么权限 2 个要素）

*权限 Rights。权限是指对一个对象采取行动的能力。例如，一个用户有权修改数据。（权限就是针对客体的，不包括“访问”）

*特权 Privileges。特权是权限和特权的综合。就是拥有一组多个最高权限的特别身份。

3.一个全面的身份管理解决方案包括以下技术：

*密码管理；*帐户管理；*配置文件管理；*目录管理；*单点登录。

4.访问控制的流程：

①Idenfication=>Authentication=>Authorization=>Access=>Accountability

即：身份标识/识别==>身份验证/鉴别==>授权==>访问==>可问责性。

AAA 服务（Authentication、Authorization、Accountability）就是为了管控 Access。

这些在第一域第一章就讲过了。

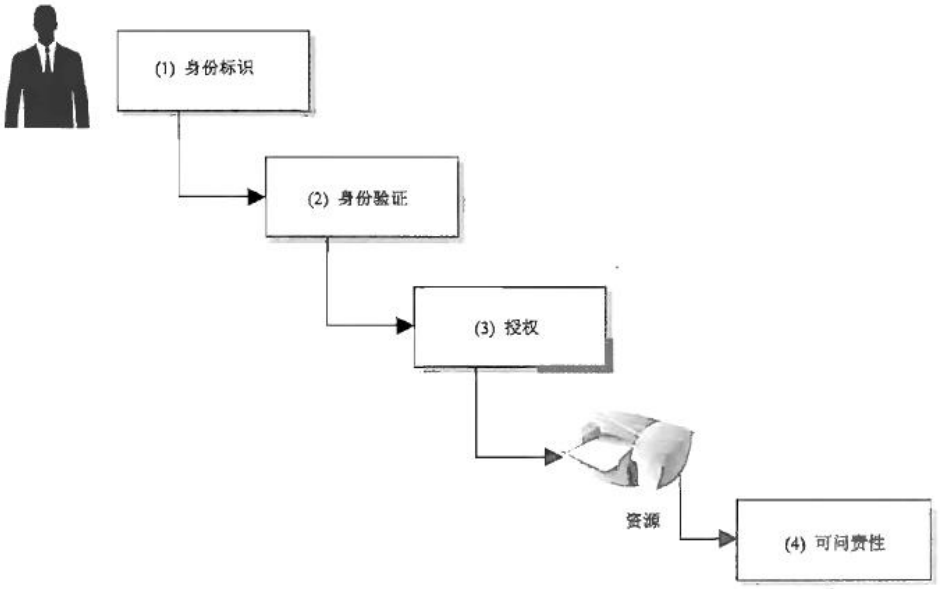


图 3-2　主体访问客体所需的 4 个步骤：身份标识、身份验证、授权与可问责性

二、密码管理

现代的大多数系统要求用户定期更改密码；为了防止暴力破解和 DDOS，多系统集成了密码多次无效尝试后被锁定的功能。密码管理系统是用来统一管理在整个企业中的密码。

三、帐户管理

账户管理系统试图简化管理跨多个系统的用户身份。后面有专门讲账户管理的生命周期。

身份管理(Identity Management,IdM)是一个广泛而又深入的术语，包括使用不同产品对

用户进行自动化的身份标识、身份验证和授权。考试中 IDM 系统一般会涉及到目录服务中的“元目录”和“虚拟目录”的内容；还会涉及到为了管理网络活动而增加的网络访问控制组件 WAM（Web access management component）；还会涉及到 3 种不同的密码更新方式：

①密码同步 Password synchronization，为了减少复杂性，自动同步不同系统的密码。

②自主修改 Self-service password reset，为了减少客服电话受理业务量，用户自己改。

③辅助修改 Assisted password reset，为了减少客服实施操作工作量，先客服验证，再让用户自己改。（一般有使用生物识别、令牌什么的）

1.这里讲下 SID

每个 Windows 用户，计算机或服务帐户具有唯一的字母数字标识符称为 SID。Willdows 安全相关的处理，例如身份验证、授权和审计，使用唯一的 SID 来标识安全主体。由于 SID 是使用在系统进程中，所以 SID 的格式对普通用户或管理员都不是很友好。AD 域帐户的 SID 是由每个 Windows 域控制器(DC)运行一个域的安全权限创建的；本地帐户的 SID 是由每个 Windows 中运行的本地安全机构(LSA)服务创建。

2.举个例子

在测试活动目录(AD)系统中可分析得到一个 SID：

S-I-5-21-4035617097-1094650281-2406268287-1981，其中：

*S：初始的 S 标识，即代表该值为 SID 字符串。

*I：SID 的版本规范。到目前为止，从未改变，一直是 1。

*5：标识符权限值。这是顶级权威发布的一个预定义 SID 标识符。这通常是 5,它表示 SECURITY_NT_AUTHORlTY。

*21-4035617097-1094650281-2406268287：这部分是域或本地计算机的标识符，在本例中它是一个域标识符。这是一个 SID 标识符创建的计算机或域的 48 位字符串。

*1981：这关联 ID(**RID**)是该 SID 的最后一部分。这 RID 可以用来唯一标识一种安全结构，这种结构与一定范围的安全授权有关，而这种安全授权产生了 SID。在 Windows 操作系统中，任何组或用户不能创建 RID 为 1000 或者更高的级别。

3.SID 唯一性

SID 的一个重要性质是其在时间和地点的唯一性。域安全机构作为跟踪的所有 SID 的颁发和吊销机构，不会允许 SID 被重用。

4.公共的 SID

公共的 SID 是一组通用用户或通用组的 SID 标识。它们的值在所有操作系统保持不变。以下是著名的 SID：

①SID：S-1-5-21domain-500

名称：管理员

描述：系统管理员的用户帐户。默认情况下，它是给予完全控制系统权限的用户帐户。

②SID：S-1-5-21domain-501

名称：访客/来宾

描述：临时的、不需要密码的用户帐户。默认情况下，Guest 帐户被禁用。

③SID：S-1-5-21domain-512

名称：域管理员

描述：授权管理域中的所有成员。默认情况下，域管理员组是已经如入到域并包括域控制器的所有计算机上 Adrninístrators 组的成员。域管理员组在默认情况下是可以创建的任何对象和任何成员的组。

基于上面列出的公共的 SID/RID 组合，我们可以知道，RID 为 500 的是系统内置的管理员帐户。这是有价值的信息，可以确定帐户是否被重命名混淆和确认其真实身份。同样，一个黑客可能去尝试确定一个帐户的真实身份。

四、配置文件管理

配置文件是与特定身份或组相关联的信息集合。除了用户 ID 和密码，用户配置文件可能包括个人信息，如姓名、电话号码、电子邮件地址、家庭地址，出生日期等。配置文件还可以包含在特定系统上特权和权利有关的信息。然而，任何用户的特定信息会随着时间的变化而变化，管理该变更过程是一个整体的身份管理中的一个重要组成部分。

当必须改变一个配置文件时，这个过程应易于管理并自动传播到关键的系统，如企业目录，和个人系统。大多数客户关系管理(CRM)系统包括使用一些工具来管理用户配置文件，可以是行政或通过自助服务方式。访问管理系统和密码管理系统中也可以实现这个功能。它有助于让用户输入和管理个人不敏感的部分新数据而不需要验证。这有助于减少实施这些改变的成本和时间，并提高准确性。

五、目录管理

集中式的访问控制系统，需要使用目录服务，它是一个集中的数据库，包含了主客体信息。公司的目录是一个集中管理与公司有关实体的各种各样数据的综合数据库，如用户、组、系统、服务器和打印机等对象的层次结构信息。目录服务的主要好处是，它是集中收集用户数据，可以由许多应用程序使用，可以避免信息复制并简化用户数据。最常用的目录协议是轻量级目录访问协议(LDAP)，其它的还有 Novell NetWare 目录服务 NDS(NetWare Directory Service)和 Microsoft 活动目录域服务(ADDS)。

目录服务就是一个为了快速读取和搜索的数据库软件，目录服务与数据库的区别：

①目录一般只执行简单的更新操作，适合于进行大量数据的检索，不支持批量更新。

②目录具有广泛复制信息的能力，从而在缩短响应时间的同时，提高了可用性和可靠性。

要搞清楚什么是元目录，什么是虚拟目录：

①元目录(meta-directories)：在中央目录中存储的必要信息，有统一视图，并定期同步；

②虚拟目录(virtual directories)：与元目录类似，区别在于元目录的目录中含有真实数据，而虚拟目录没有，虚拟目录只是指向实际的数据库。

1. X.500

X.500 系列通信协议是由国际电信联盟(ITU-T)在 90 年代初开发，最初被称为 ISO/IEC 9594-1：2008，现在是 ISO/IEC 9594-1：2014。它由四个不同的协议组成：

①目录访问协议(DAP)，主协议；

②目录系统协议(DSP)；

③目录信息屏蔽协议(DISP)；

④目录操作绑定管理协议(DOP)。

信息在 X.500 目录中被组织成一个层次数据库，所有资源的都有一个专有名称/可区分名(**DN**)，它提供在 X.500 数据库中的完整路径，可以找到其中一个特定的条目。X.500 还支持一个相对专有名称(**RDN**)，它提供了一个特定项目的名称，而不附加完整路径的组件。目录内的客体由目录服务管理。目录服务允许管理员配置和管理如何在网络中进行身份标识、身份验证、授权和访问控制。目录内的客体通过名称空间标记和标识。

举个例子：

在 Windows 环境中进行登录时，你会登入一个域控制器(Domain Controller,DC)，它的数据库中具有一个层次化目录。这个数据库运行一个目录服务(Active Directory)，活动目录)，该服务组织网络资源并执行用户访问控制功能。因此，一旦成功登入域控制器，根据活动目录的配置，你就可以访问某些网络资源(如打印服务、文件服务棒、电子邮件服务器等)。

目录服务如何让这些实体保持有序运行呢?这就需要使用名称空间。每种目录服务都采用某种方式标识和命名它们所管理的客体。在基于 X.500 标准的、由 LDAP 访问的数据库中，目录服务为每个客体分配可区分名/专用名称(Distinguished Name, DN)。每个 DN 代表与某个客体有关的一组属性，并且作为一个条目存入目录。

下面讲的术语是按 LDAP 的标准来的：

①**DN** 可区分名 Distinguished Name；是 LDAP 记录项的名字(唯一)，每一个 LDAP 记录项的 DN 是由两个部分组成的：相对 DN（RDN）和记录在 LDAP 目录中的位置，反正好多属性值。DN 的读法和 DNS 主机名类似。

②**CN** 通用名称 Common Name；

③**DC** 域组件 Domain Component；

④**OU** 组织单元 Organization Unit；用来表示公司内部的机构：销售部、财务部，等等。

⑤**RDN** 相对专有名称；RDN 是 DN 中与目录树的结构无关的部分（没有路径）。在 LDAP 目录中存储的记录项都要有一个名字，这个名字通常存在 CN（Common Name）这个属性里，作为 RDN 的基础。如果我把最喜欢吃的燕麦粥食谱存为一个记录，我就会用 CN=Oatmeal Deluxe 作为记录项的 RDN。

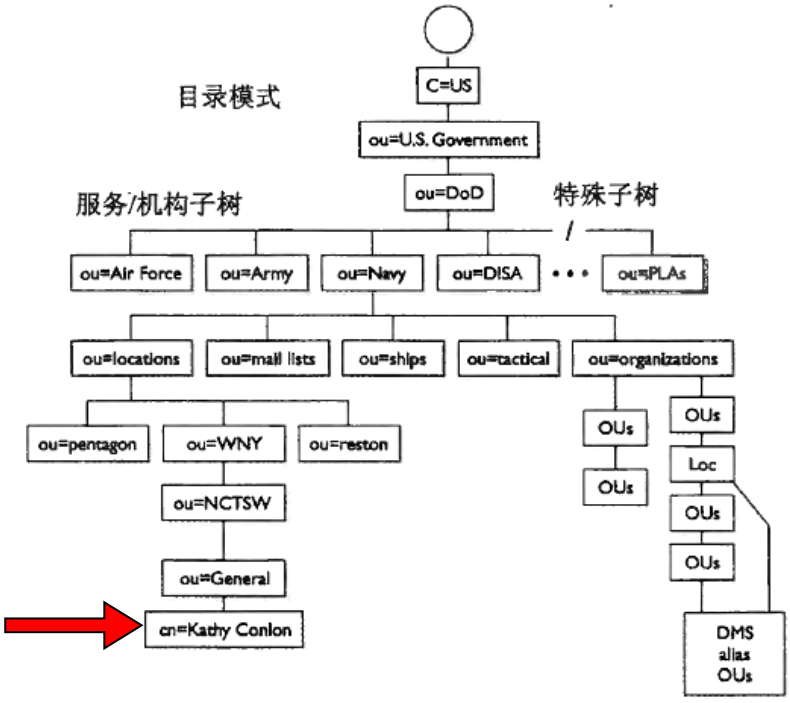
DN=DC+CN+OU，RDN=CN。

在基于 X.500 标准的数据库目录中，下面的规则用于组织客体：

- 目录采用树结构，使用父-子配置来组织条目。
- 每个条目都具有由某个特定客体的属性组成的唯一名称。
- 目录中所使用的属性由预定义模式规定。
- 唯一标识符称为可区分名。

预定义模式描述了目录结构和目录内可以使用的名称以及其他内容(第 10 章将详细介绍模式和数据库组件)。

下图说明了一个客体(Kathy Conlon)如何拥有 ou=General ou=NCTSW ou=pentagon ou=locations ou=Navy ou=DoD ou=U.S. Government C=US 的属性。



需要注意的是，OU 表示组织单元。OU 用作其他类似 OU、用户和资源的容器，并且可以提供父-子(有时也称为树-叶)组织结构。

2.轻量级目录访问协议(LDAP) Lightweight Directory Access Protocol/最重要

与 X.500 不同，LDAP 支持 TCP/IP。许多目录服务建立在轻量级目录访问协议(LDAP)基础上。例如，Microsoft 动态目录域服务就是以 LDAP 为基础的。公钥基础设施（PKI）用于管理和传输数字证书，它就要使用 LDAP，LDAP 也用于实现单点登录功能。下面讲的密钥管理中心（KDC）也要用到 LDAP。

LDAP 是各种网络服务、主体、客体和资产的名录清单。用户、客户和流程可以搜索目录服务找到所需系统或资源存储的地方。访问控制系统经常会用到多个域和信任关系。**安全域**是主客体的集合，共用一个安全策略，单个域可以独立于其他域单独操作。**信任**是域和域之间所建立的安全桥梁，允许用户从一个域访问另一个域中的资源。

LDAP 使用分层树结构的目录条目。与 X.500 一样，LDAP 条目支持 DN 和 RDN 概念。DN 属是一个实体的 DN 名称，RDN 只有名称不包含路径。数据库中的每个条目具有一系列名称/值对，来表示与每个条目相关联的各种属性。LDAP 条目的常见属性包括（具体见上面的图和示例）：

①DN 可区分名；②CN 通用名称；③DC 域组件；④OU 组织单元；⑤RDN 相对专有名称

LDAP 使用 C/S（客户机/服务器）体系结构，客户端发出请求访问 LDAP 服务器，服务器将响应请求的结果返回到客户机。LDAP 使用 TCP 端口 389 进行通信。如果需要高等级的安全，第三版的 LDAP 协议支持使用 TLS 加密通信（636 端口）。全局编录服务器使用 TCP 3238 端口（不加密）、3269 端口（加密）。

3.活动目录域服务(ADDS)

活动目录域服务，通常被称为 AD 域或 ADDS，是 LDAP 协议基于 Microsoft 环境的实现。通过使用附加的插件服务，LDAP 目录可以通过许多其他系统，包括 UNIX,Linux 和甚至大型机环境中使用。ADDS 提供了在一个企业范围的用户和系统服务中心的认证和授权功能。ADDS 有能力实现强制执行组织的安全和跨企业配置策略。

ADDS 在命名结构上使用了 LDAP。与 LDAP 一样，ADDS 使用层次框架的一种体系来存储信息。ADDS 目录被组织成**树**和**森林**。森林是所有的对象及其关联属性的集合，树是一个或多个增加了一个森林内的安全域逻辑分组。域在 ADDS 是他们的 DNS 名称标识。在 ADDS 数据库的对象由组织单位分组。

4. X.400

X.400 协议支持两个主要的功能：消息**传输**和消息**存储**。X.400 的地址包含一系列用分号分隔的名称/值对。

一个典型的地址组件包含：

组织名称(O)；组织单元名称(OU)；指定名称(G)；缩写(I)；姓(S)；国家名(C)。

下面重点讲单点登陆

六、单点登录 Single Sign-On

单点登录(SSO)是一种集中式访问控制技术，允许一个主体只在系统上认证一次并且可以不用认证身份而访问多个资源。但是，一旦账户被破解，那么恶意主体就会拥有不受限制的访问权限。常用的单点技术有：

*基于脚本的单点登陆：代替用户与应用进行交互，去登陆其它系统。堡垒机就用的这个。

*Kerberos：由 KDC 来发“票”，对称加密。

*SESAME：要用到特权证书 Privileged Attribute Certificates (PACs)和鉴权服务 Privileged Attribute Server (PAS)。

*Security domains：主、客体都在同一密级的域时里，不存在越权了。

*Directory services：所有资源按标准进行命名。

*Thin clients：客户端搞定。

1. Kerberos（希腊神话里的 3 头看门狗）（必考）

这是麻省理工大学开发的身份验证技术，在 UNIX、WINDOWS、LINUX、MAC OS 等操作系统都使用了，是开放的免费的协议，具有保护网络的三个要素：身份验证，授权和审计（AAA）。它采用第三方实体来验证身份，是 C/S 架构（客户端/服务器），提供单点登录解决方案，可以用在单机登录、本地 LAN、远程访问等。现在的 Kerboros 5 版本依赖的是对称密钥加密的高级加密标准(AES)协议，使用端对端安全机制保障认证通信的机密性和完整性，有助于预防窃听和重放攻击。它的体系包括几个重要元素：（如果不理解这些要素，先看看 Kerboros 的

认证流程就好）

Kerberos 用的是 KDC，另外有一个技术是 PKI，用到了 CA、RA 什么的，这里不讲了，都学完了建议联系起来理解。

①委托人 principal（主体/客体）

任何主体（用户、应用程序）和任何客体（数据、文件）都是委托人，委托人之间的访问信任必须通过 KDC 来建立，整个系统只是 KDC 是完全可靠可信的；客体接不接受你的访问，全看你有没有 KDC 给你的“票”，没票免谈。

为了安全、方便的保存和使用那么多委托人的账户数据，就需要所谓的“目录访问服务”了，即账户数据库。那么多的不同部门、不同系统的委托人，一般会分组来管理，这就是所谓的域了（realm）；KDC 可以对多个不同的域提供身份认证服务。

强调一下，每个委托人都必须安装 Kerboros 的客户端软件的，不然无法实现与 KDC 的验证，而且那个所谓的每个委托人与 KDC 之间的唯一的“对称密钥”是由这个客户端和 KDC 同步生成的。

②密钥分发中心 The key distribution center (KDC)

KDC 是提供身份认证服务的可信第三方。所有委托人（用户和服务）都在 KDC 做了注册，并由 KDC 维持一个属于该委托人的密钥（所谓的对称密码学）。委托人的身份通过这个密钥来向 KDC 来验证（不需要发送真实的密码）。KDC 与委托人之间传输的只有密钥和票据。

③Kerberos 身份认证服务器（TGS+AS）KDC=TGS+AS

身份认证服务器就是 KDC 的服务器，是 KDC 功能的实现，包括 2 个重要部分：票据授予服务/票证发放服务器 TGS（ticket-granting service）和身份认证服务 AS（authentication servi）。TGS 也就是 KDC 服务器，发票的；AS 对票证真实性和实效性进行验证，验票的。

④授予票证 ticket-granting ticket（TGT）

TGT 是用户登录时，KDC 验证完自己身份后派发的一个**根票据**，相当于是委托人的“身份证”，拿到 TGT 就证明我是有身份的人了（证明了我是我自己，我妈是我妈）。它被叫做“票证授予的票证”，意思是要想被授予票证去访问某个资源，你得先有这个证才行。TGT 进行了加密，包括一个对称密钥、一个过期时间和用户的 IP 地址；TGT 的有效期一般为几个小时；主体在请求得到访问某个客体的票据时，先向 KDC 出示自己的 TGT。TGT 就相当于获得了“护照”，而下面的 ST 就相当于去某国的“签证”。

⑤票据 ticket（ST）

票据就是票，也有称为票证，还有的称为服务票据(ST)service ticket。是一个加密的信息，是主体访问客体的唯一凭证，由 KDC 的 KGS 生成并发给主体，代表给主体被授予了访问某个客体的权限。Kerberos 的票据有特定的寿命和使用参数，一旦票据到期，就得续期或者重新申请。也就是说 KDC 给了你什么票，你就能去什么场，要想去很多场地，就要有很多票。

Kerberos 用户的登录过程（目的是证明自己，拿到 TGT）：

1.用户向客户端输入用户名和密码。

2.客户端使用 AES 加密用户名，然后传输至 KDC。（AES 使用客户端的初始密钥）这个过程其实也可以不加密，直接发送出去，并不影响安全。

3.KDC 的 AS 负责验证身份，它向账户数据库验证用户名。

4.用户名验证通过后，KDC 的 AS 生成一个对称密钥，再生成一个时间戳的授予票证(TGT)，并向账户数据库读出用户密码；然后用对称密钥加密 TGT，再使用用户密码的散列值来加密对称密钥。

5.KDC 将加密的对称密钥和 TGT 传输给客户端。

6.客户端使用用户密码的散列值来解密对称密钥，用得到的对称密钥再解密 TGT。客户端安装 TGT，一直使用至其期满。如果用户不知道自己的密码，就得不到对称密钥，也就得不到 TGT，而整个过程密码并不在网上传播，是通过散列认证的。

用户请求访问资源的过程（目的是获取授权，访问服务或数据）：

1.客户端将 TGT 发送回 KDC，同时请求访问某个数据或服务。

2.KDC 验证 TGT 的有效性，对比查看其访问控制表，确认用户是否拥有所请求资源的访问权限。

3.KDC 的 TGS 生成一个服务票据（ST），就是票据，然后发送至客户端。这个票据 ST 里有这些信息：一是 TGS 生成的一个会话密钥，用于随后主体（客户端）与客体（服务）间建立加密通信；这个会话密钥是加密后才发出来的，一个用主体的密钥加密，一个用客体的密钥加密；此外，票据里还有 1 个身份验证器，包含这些信息：主体的身份标识（用户名）、IP、序列号和时间戳。（注意，这第一个身份验证器不用发给主体，直接发给客体就好）

4.客户端得到票据，先解密出会话密钥，用后随后的通信加密；再把自己的身份信息写入票据，这样票据有了第 2 个身份验证器（身份验证信息都是用会话密钥加密的）；最后把新的票据发送给要访问的服务器或主机（客体）。

5.服务器或主机（客体）得到票据，先解密出会话密钥（如果能解密出来，说明这个票据是可信的，是来源于 KDC 的，因为只有 KDC 知道它的密钥）；然后用会话密钥解密分别来自主体和 KDC 的 2 个身份验证器，如果是一样的，说明对方身份是正确的。

6.一旦票据被认证合法，Kerberos 的任务就完成了。用户客户端与服务器或主机随后建立加密通信会话，开始数据传输。身份验证信息里的时间戳和序列号都可以防范重放攻击。

这里面的考点很多，其中秘密密钥是委托人与 KDC 之间用的，会话密钥是主体访问客体时用的，两者都是 KDC 随机生成再分发的。

Kerberos 的缺点：

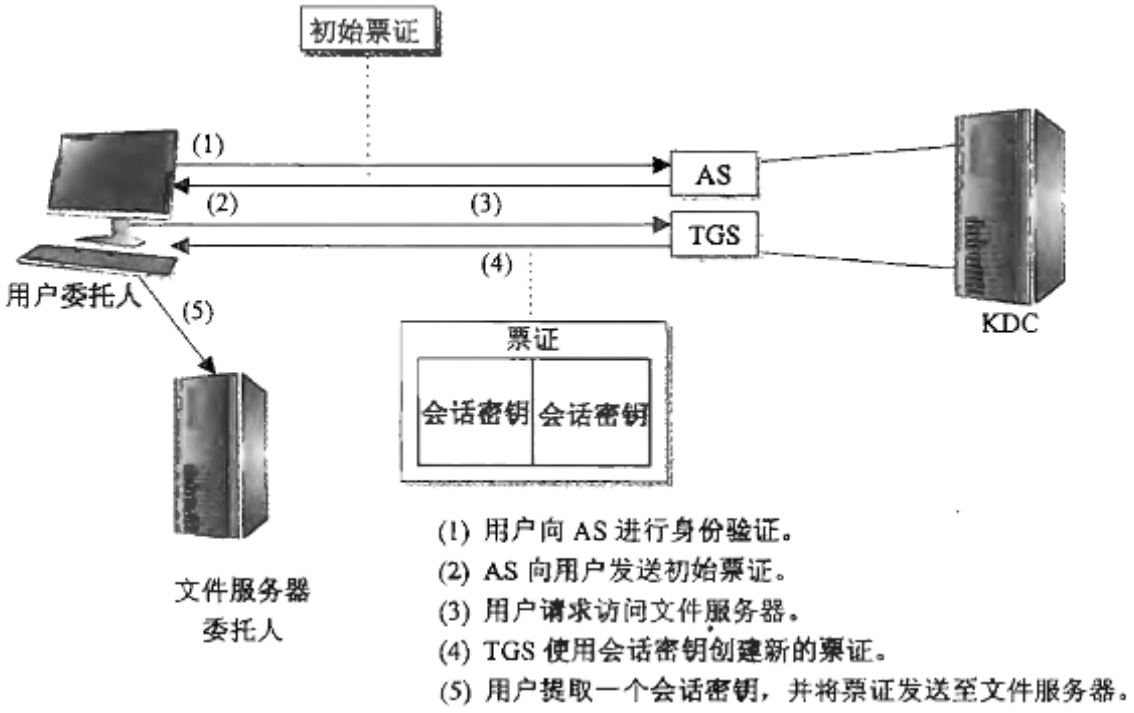
①存在单点故障。如果 KDC 被破解，所有系统的秘钥也都会被破解；如果 KOC 离线，那么就无法完成身份认证过程。

②有严格的时间要求。即所有的系统彼此要在五分钟内同步时间，如果一个系统不同步或时间被改变了，以前发出的 TGT 将不再是有效的，系统将无法接收任何新的票据。实际上，客户端将被拒绝访问任何受保护的网络资源。反正客户端必须要与 KDC 服务器的时间同步。

③KDC 的性能要够好，能满足大量认证需求，并且是可扩展的，不然就跑不动了。

④不加密通信流量。

⑤其密码或密钥可能遭受暴力破解/蛮力攻击/字典攻击。



2.其它单点登陆的技术

①欧洲安全多环境应用系统(SESAME) Secure European System for Applications in a Multivendor Environment

这是一个基于邀请的认证系统，其开发是为了解决 Kerberos 的缺点。不过，最终还是新一代的 Kerberos 更好，SESAME 已经不再用了。SESAME 混合使用对称密钥和非对称密钥，而 Kerberos 只用了对称密钥。

Kerberos 通过使用票证来让主体通过客体的身份验证，而 SESAME 则使用特权属性证书 PAC(Privileged Attribute Certificate),PAC 包含主体的身份、对客体的访问能力、访问时间段以及 PAC 的生命期。PAC 具有数字签名，因此客体能够确保其来自可信任的身份验证服务器，这种服务器被称为特权属性服务器 PAS(privileged Attribute Server)。PAS 扮演与 Kerberos 内的 KDC 类似的角色。用户成功通过身份验证服务的身份验证之后就会得到一个要提交给 PAS 的令牌。PAS 随后为用户生成一个 PAC ，该 PAC 用于提交给要访问的资源。

②凭证库思想(Krypto Knight)

是 IBM 开发的一个基于邀请的认证系统。它与 Kerberos 相似，但是使用对等认证而非第三方认证。KryptoKnight 被纳入 NetSP 产品。不过，SESAME、KryptoKnight 和 NetSP 从未盛行，并再也不会被广泛使用。

这里讲的“基于邀请”是指“ticket-based”，就是基于“邀请函、请帖”，即“票”。

③OAuth (意为公开认证)和 OpenID 是应用于网络单点登录的较新的例子。

OAuth 协议是一个开放标准，它与 HTTP 协作，允许用户以单一账户登录。例如，谷歌支持 OAuth 2.0。

Open ID 也是一个开放标准，但是它由电脑软件公司 the OpenID Foundation 保持，并不是 IETF RFC 标准。OpenID 可与 OAuth 共同使用，也可单独使用。

区别与联系：

OAuth>OpenID；OpenID 是身份验证 Authentication；OAuth 是授权 Authorization。

前者是网站对用户进行认证，让网站知道“你是你所声称的 URL 的属主”；后者其实并不包括认证，只不过“只有认证成功的人才能进行授权”，结果类似于“认证+授权”了。OAuth 相当于：A 网站给 B 网站一个令牌，然后告诉 B 网站说根据这个令牌你可以获取到某用户在 A 网站上允许你访问的所有信息。

3.集中式单点登录系统的缺点

①用户的凭证都是由一个密码保护，如果有人破解了，那么攻击者就能访问整个系统中所有应用的权限。

②所有的用户凭证和身份验证信息都存储在一个数据库中，系统需要实施强大的监控和检测，以确保任何问题都捕获并尽快处理。

B.2 单/多因素认证（例如： 因素、强度、错误、生物识别）

主体是活动的实体，它通过访问被动客体去获得客体的信息或数据。主体可以是用户、程序、进程、文件、计算机或者去访问资源的任何东西。当通过授权，主体就可以修改客体。客体客体是提供信息给话动主体的被动实体。**客体**可以是文件、数据库、计算机、程序、进程、打印机和存储介质等。通常用“用户”一词代替主体，用“文件”一词代替客体。

1.认证因素 Authentication Factors

一般严格的身份验证多是多因素的，需要几个东西一起来证明身份。认证因素主要有 4 类：

①类型 1：Know 你知道什么？消息验证。例如：密码、个人标识码(PIN)或密码短语。

②类型 2：Have 有拥有什么？所有权验证。例如：智能卡、硬令牌、记忆卡和 USB 驱动器。智能卡和记忆卡之间的主要差异是：智能卡有处理数据的能力，而记忆卡只用于存储信息。

③类型 3：Who 你是什么？特征验证。指某个身体部分或人的物理特征，例如：指纹、语音、波纹、视网膜、虹膜、脸、掌纹和手型等；当然还包括你做什么？如：签名和击键力度。

其实还有第 4 因素：你在哪里？地址验证。例如终端 IP、电话号码或国家等物理位置信息，只有和其它因素联合使用时才会有效。

当使用两个相同的因素，系统的强度并不会超过只单独使用其中一个因素的系统强度。

2.密码

密码其实很好理解，弱密码强密码什么的，这里补充些别的内容。

①密码短语 Password Phrases

比基本密码更有效的密码机制是密码短语，类似于密码字符的字符串，但对于用户具有独特的意义。为了简化记忆，密码短语往往是修改过的自然语言语句。例如：“1 passed the CISSP exam”会被转换为这样的密码短语“IP@$$edTheCISSPEx@m”。密码短语难以被破解，还很容易记住。

②认知密码 Cognitive Passwords（考点）

认知密码是另一种密码机制，通常是一系列问题，一般用做帐户的密保问题，例如：你的生日是哪一天?你喜欢的运动是什么?等等。就像是找回密码时用的密保问题，但密保问题并不是一个密码概念，更不是题目中的正确答案。有的地方也会出现基于知识的认证方法 Knowledge-based authentication，也用这种密保问题。

3.智能卡和令牌 Smartcards and Tokens

智能卡和信息就是第二类认证因素：你拥有什么？

①智能卡

智能卡有多种形式，最新的智能卡包含一个微处理器和一个或多个证书。证书用于非对称加密，比如加密数据或数字签名的电子邮件等。智能卡既可以进行身份识别，也可以进行身份认证。但卡容易丢失，使用智能卡时大多会要求用户再设置另一个身份认证因素，如 PIN 码。

②令牌

一次性密码 **OTP**(One-Time Password)也称为动态密码，用于身份验证，只能使用一次。令牌和密码短信都是，现在金融网站都用软令牌了（通过短信，灵活方便自控）。

令牌或硬件令牌是一种密码生成设备，用户可以随身携带，网上银行用的特别多，形式也很多。类型有两种：同步动态密码令牌，和异步动态密码令牌。

同步动态密码令牌创建同步动态密码的硬件令牌是基于时间的（或基于计数器/事件型生成器），并与身份认证服务器保持同步。他们定期生成一个新密码，如每隔 60 秒。这也就要求令牌和服务器必须有精确的时间。

异步动态密码不用时间，依据算法和递增计数器生成密码。有些令牌则是由用户输入认证服务器提供的 PIN 码后，会生成一次性密码。

最后讲讲**软令牌**：

软令牌存储在计算机上，需要通过身份验证的第二个因素来激活，如 PIN 密码或生物特征。相较于硬件令牌，软令牌比较便宜，易于实现和管理，能避免一些物理安全风险。然而，软令牌也很容易受到计算机病毒，中间人攻击，钓鱼，和其他软件的攻击。使用软令牌要遵循以下准则：

①私钥必须是不可导出的。

②密钥必须是加密存储的。

③种子记录和初始密码短语的分发必须加密。安装软令牌软件通常有两条信息：种子记录和密码，两者都需要安装和初始化令牌生成引擎。这两条信息，如果被未经授权的用户捕获，可能导致未授权软件的安装和未经授权的使用。

④每次使用软令牌的用户必须进行身份验证，令牌必须被激活。

⑤令牌时限必须少于 2 分钟。

⑥软令牌软件的密码应符合密码管理原则

⑦审计所有软件令牌的访问。

⑧使用软件令牌之前，必先安装最新的防病毒软件。

⑨始终使用 FIPS 140-2 验证的加密模块。其加密模块必须被验证，以满足 FIPS 140-2 第 1 级标准。

③ISO/IEC14443，智能卡标准

14443-1——物理特性

14443-2——射频功能及信号接口

14443-3——初始化和零冲突

14443-4——传输协议

4.生物识别Biometrics

生物识别属于第3类身份认证因素，即，你是什么？

①生理识别方法。包括指纹、面部扫描、视网膜扫描、虹膜扫描、手掌扫描、手形和语音模式。

②行为识别方法。包括动态签名和击键模式(击键力学)，也称为你所做(something-you-do)的身份认证。

指纹都很普通，主要讲下别的：

*视网膜扫描（Retinal Scanning）的是眼睛后方血管的图案，它会泄露个人健康状况。视网膜没有虹膜那么多的生物多样性，也容易变化。

*虹膜扫描（Iris Patterns）是最精确的生物认证形式，扫描的是瞳孔周围的有色区域，它一生都不会变。它可以区分同卵双胞胎的，甚至同一个人的左右眼。

*手掌扫描（手掌特征或手掌纹理)是用近红外光测量手掌的静脉。

*手部外形识别手部的物理尺寸，包括手掌和手指的宽度与长度，即手的轮廓，它不能捕捉指纹细节或静脉模式。这种方法比较难识别出一个人的独特性。不好用。

*声音识别依靠一个人说话的声音特点，称为声纹。也不好用。

*签字力度识别主体如何书写字符串，依赖于用笔的压力、笔划方式、笔划长度以及提笔时间点。

*击键模式(击键力度)通过分析抬指时间与按压时间来分析主体使用键盘的方式。误差比较大。

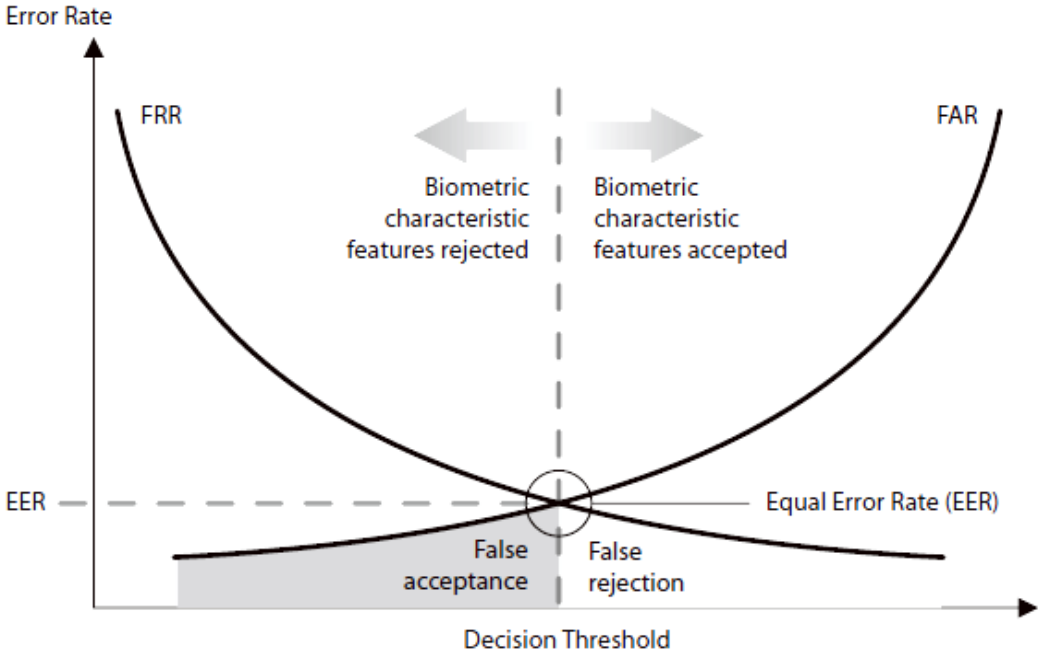
生物识别的灵敏度极易产生2种错误：误报(false positive)或漏报(false negative)，为了提高准确度，有几个重要的指标参数（一拒二收，开始是拒绝的，后来接受了）：

①**一类错误/拒绝** Type 1 Error，即错误拒绝率(**FRR**) false rejection rate，正确的主体被拒绝的概率，就是识别太敏感了，动不动就不认。

②**二类错误/滥收** Type 2 Error，即错误接受率(**FAR**) false acceptance rate，错误的主体被接受的概率，就是识别太模糊了，什么都认。

③**交叉错误率**(**CER**)/相等错误率(**ERR**)。就是两类错误相同时的概率指标，代表了系统经调校后的综合识别能力水平，最低越好。

当然，根据组织的需求，可以让某一类错误多出些，另一类最好不出。



B.3 可追溯性 Accountability

可追溯性/可问责性/审计是能够确定谁或什么是负责的操作，并可以追究责任。强大的身份识别，认证，审核和会话管理的背后最终驱动力之一就是问责制。

问责在很大程度上依赖于不可抵赖性，但它们还是有区别的。不可抵赖性是与信息保障密切相关的一个话题；否定是否认一个动作，事件，影响或结果；不可抵赖性是确保用户不得否认行动的一个过程。问责在很大程度上依赖于不可抵赖性，以确保对用户的流程和行动可以被追究责任。

一、授权和可问责性 Authorization and Accountability

①授权。依据主体的证明身份授予其访问客体权利。

②可问责性/可追溯性。在执行审计时用户和其他主体要对自己的行为负责。

补充知识：

授权蠕动(authorization creep)

当雇员在一家公司长期工作时，他们会从一个部门调动到另一个部门，因此常常被赋予越来越多的访问权限和许可。这种情况通常称为授权蠕动(authorization creep)。

擦洗(scrubbing)

攻击者经常会删除保存其犯罪活动信息的审计日志(删除审计日志中特定犯罪数据的行为称为“擦洗(scrubbing)”。

二、AAA 协议

提供**认证、授权和可问责性**的协议叫做 AAA 协议。authentication, authorization, and accounting(最后一个可问责性有的地方描述为“审计 Audit”,效果和意思都是一样的)。AAA 协议就是指功能完备的严格的访问控制协议。他们提供集中式访问控制，附带例如虚拟专用网(VPN)和其他类型的网络访问服务器的远程访问系统。他们可以保护内部局域网认证系统和其他服务器遭受远程攻击。当使用一个单独的系统进行远程访问时，对系统的成功攻击只会影响远程访问用户。一些常见的 AAA 协议有 RADIUS、TACACS+ 以及 Diameter。上一章节“单点登

陆里”讲的 kerberos 也是 AAA 协议。

下面讲的是集中式“访问控制管理”centralized ACA,access contrl administration。分散式 decentralized 的比较简单，不讲了。

1.RADIUS（Remote Authentication Dial-In User Service）

远程认证拨号用户服务器(RADIUS)主要用于远程连接的身份认证。RADIUS 服务器为多个远程访问客户端提供 AAA 服务。许多互联网服务提供商(ISP)使用 RADIUS 进行身份认证。用户可以在任何地方访问 ISP。RADIUS 采用用户数据报协议(UDP)，并只加密交换密码协议，不会加密整个会话，但可以使用附加协议来对数据会话进行加密。RADIUS 是一个集中认证机制，提供认证，授权和计费。使用 802.1x 是的一个改进形式，这是一个 EAP 和 RADIUS 的组合，在发送用户标识是使用明文，但密码是加密的。

总的来说，RADIUS 有以下问题。它：

①已成为密码攻击的受害者，已经被重放攻击成功攻击。

②缺乏完整性保护。

③只有特定字段使用加密（仅密码加密）。

2.TACACS+（Terminal Access Controller Access Control System）

终端访问控制器访问控制系统(TACACS)是 RADIUS 的一种升级和替代，**思科**提出的商业协议。后来推出了扩展 TACACS （XTACACS)，并将其作为一项专有协议。然而，TACACS 和 XTACACS 如今都不常用。后来，又推出了 TACACS+，并被作为一个开放的协议，成为了三个协议中最常用的一个。

①TACACS 将它的身份验证和授权过程组合在一起。（使用固定密码）

②XTACACS 将身份验证、授权和审计过程分隔开。

③TACACS+则在 XTACACS 基础上采用**双因素**用户身份验证。（使用动态(一次性)密码）

TACACS+（网络设备查询服务器验证密码）将认证、授权以及可问责分为独立的流程，并可以在三个独立的服务器上进行托管。TACACS+可以加密所有的认证信息，而不仅仅像 RADIUS 一样只是加密密码。TACACS 和 XTACACS 使用的是 UDP 端口 49，而 TACACS+使用的是传输控制协议 TCP 端口 49，为数据包的传输提供了更高的可靠性。上面 2 个的区别：

	RADIUS	*TACACS/XTACACS*	*TACACS+*
数据通信	UDP	UDP：49	TCP：49
数据加密	仅加密传输的用户密码	唔知	加密客户端-服务器全部流量
AAA 功能	集中整合合认证和授权	前者整合/后者分离	验证、授权和审计过程分隔开
协议支持	仅 PPP 连接	唔知	还支持 IPX、AppleTalk、NETBIOS
挑战响应	对所有 AAA 活动仅执行一次挑战响应认证（单）	唔知	对各项不同的 AAA 活动分别执行挑战响应认证（多挑战）

3.Diameter

基于 RADIUS 和 TACACS+的成功应用，又开发出了一个名为 Diameter 的 RADIUS 的增强版本。它支持多种协议，包括传统 IP、移动 IP、IP 传真和 IP 语音(VoIP)。因为其支持许多附加的命令，尤其在支持漫游服务情况下特别受欢迎，例如无线设备和智能手机。虽然 Diameter 是 RADIUS 的升级版本，但是其并不兼容 RADIUS。

Diameter 使用的是 TCP 端口 3868，或流控制传输协议(SCTP)端口 3868，相比于 RADIUS 使用的 UDP 端口来说，提供了更好的可靠性。它也支持网际安全协议(IPsec)和传输层面安全协议的加密。Diameter 这个名称也意味着 Diameter 要比 RADIUS 好两倍。

前面讲的 RADIUS 和 TACACS+都是客户端/服务器协议，服务器只能被动作出响应。而 Diameter 是一个**对等协议**，允许任何一端发起通信。只要考题里涉及了 **VoIP** 或者**对等服务**，那一定是选 Diameter 集中访问控制系统了。

4.总结：

RADIUS：开放 C/S，仅 PPP 拨号，UDP，仅加密密码，AAA 整合，远程审计，单挑战，256AVP。

TACACS：身份验证+授权=》不分离，UPP。

X-TACACS：扩展的，AAA 分离即隔离=验证-授权-审计。

TACACS+：C/S，动态密码，多网络协议，TCP，全加密，AAA 分离，更多 AVP，多挑战。

Diameter：对等通信，TCP，移动 IP，VoIP，不兼容，2^{32}AVP，**AVP** 是指属性值对。

B.4 会话管理（例如：超时、屏保）

很简单。区分桌面会话（人面界面）和逻辑会话（后台通信）。

B.5 身份注册与证明

身份验证是收集和验证身份信息的过程，验证某人所请求的帐户或凭证确定是其本人。

1.电子认证

电子认证(E 认证)是建立在信任用户提交电子身份给信息系统的过程。

2.美国联邦机构之间的信任

在美国，联邦机构负责核实或验证个人身份的问题凭据，一旦某人或主体的信任被认可，就会建立和绑定身份证明到个人身份验证(PIV)证书（相当于 kerberos 里的 TGT），有了证书，就可以被整个联邦企业信赖和接受。

3.联合身份管理

在联合环境中，联盟中的每个组织应遵守的一套共同的政策，标准和程序，并配置和管理用户身份标识，身份验证，授权信息。这样，用户可以实现跨平台的单点登陆。联合身份管理系统使用两种方法来实现信任链：一是交叉认证，二是第三方认证。

4.交叉认证模式

每个组织都必须单独证明每一个其他参与组织都值得信任(任意两个之间都要确认可信)。这样，一旦组织的数量达到几个以上，组织之间的信任关系会急剧增加（类似于对称密钥的管理）。

5.可信的第三方模型

很多集中式的身份认证都是这样的。PKI 什么的。

B.6 联合身份管理（例如：SAML）

一、联合身份管理与 SSO

一个完整的体系可以用 Kerberos 来实现单点登陆，但如果在互联网上或者其它很多异构集成的系统环境里，只能靠联合身份管理来实现单点登陆了。像使用 QQ、微信就可以登陆各

大论坛什么的，这里要重点讲各种系统间交互通信使用的语言了：

其中 SAML 主要用于单点登陆；XACML 主要用于软件定义网络。

①GML=>SGML=>**HTML**

超文本标记语言超文本标记语言(HTML)用于展示静态网页,它源自通用标记语言(GML) 和标准通用标记语言（SGML)。

②XML=>**SAML**

可扩展标记语言(XML)不仅是对数据显示方式的描述，它实现了对数据本身的描述。**安全断言标记语言(SAML) Security Assertion Markup Language** 是一种基于 XML 的语言，也称安全声明标记语言。普遍用于联合组织之间交换认证和授权(AA)信息（提供身份验证信息给联合身份管理系统，即以标准格式发送诸如密码、密钥或者数字证书等身份验证消息），为浏览器访问提供单点登录(SSO)功能。SAML2.0 实现基于 Web 的认证和授权方案，包括单点登录(SSO)。

SAML 规范定义了三种角色：User 委托人　IDP 验证　SP 服务

*委托人(通常是用户) principal。

*身份提供者(IDP) identity provider。

*服务提供商(SP) service provider。

当使用 SAML，委托人请求来自服务提供商的服务。服务提供商请求并获取身份提供者的身份声明。在此声明的基础上，服务提供商可以进行访问控制决策。

SAML 数据可以通过不同类型的协议传输，但常用的一个协议是简单对象访问协议(Simple Object Access Protocol)。**SOAP** 是一个规范，规定了如何以结构化方式交换与 Web 服务有关的信息。它提供了基本的消息框架，使得用户可以请求一个服务，同时，该服务也可以提供给该用户。比如，你需要与你公司的顾客关系管理系统进行交互，假设该系统由供货商 A.com 托管和维护。你登录公司的门户网站后点击 A.com 的链接，你公司的门户便会接受这个请求和你的身份验证数据，然后以 SAML 形式打包，把数据封装进入一个 SOAP 消息。这个消息通过 HTTP 连接发送给 A.com 供应商网站，一旦你的身份得到验证，你便会看到公司顾客数据库的内容了。以这种方式使用 Web 服务也使得组织可以提供面向服务体系结构 **SOA**(Service Oriented Architecture)的环境。

③XML=>DSML=>**SPML**

服务供应标记语言(SPML) Service Provisioning Markup Language 是基于 XML 的新框架，但是出于联合身份单点登录目的，专门设计用于用户信息交换（交换供应数据 ）。SPML 基于**目录服务标记语言(DSML) Directory Service Markup Language**，而 DSML 可以 XML 格式显示基于轻量级自录访问协议(LOAP)的目录服务信息。

SPML 由 3 个主要实体组成：RA 请求　PSP 响应　PST 供应

*请求机构 RA(Requesting Authority)：请求建立新账户或对已有账户进行修改的实体。

*供应服务提供者 PSP(provisioning Service Provider)：响应账户请求的软件。

*供应服务目标 PST(provisioning Service Target, PST)：在被请求要修改的目标系统上执行配置活动的实体。

④XML=>**XACML/EACML**

扩展访问控制标记语言(XACML) Extensible Access Control Markup Langua 用于在 XML

格式内定义访问控制策略（SAML 发送身份验证消息，但并判断用户的访问权限），并且它通常实现基于角色的访问控制。XACML 既是一个描述访问控制策略的语言，又是一个以标准化方式解释和执行策略的处理模型。XACML 有助于给联盟中所有成员提供保证，保证他们向不同角色授权相同级别的访问。

XACML 也有几个重要的组件：主体　行动　资源

*主体单元(请求实体) requesting entity。

*资源单元(被请求实体/客体) The requested entity /Resource unit。

*行动单元(访问类型/权限参数) types of access。

⑤总结：

GML>SGML>HTML：**HTML 的演变过程**

SPML(Service Provision)：服务供应：改账户：管理异地账户，交换应用数据，RA>PSP--PST

SAML(Service Assertiong)：断言标记：发账户：SOAP+SOA 交换身份验证和授权数据

XACML/EACML(extensible Access Control)：扩展访问：加权限：加上安全策略

SOAP(Simple Object Access Protocol)：Web 服务的信息交换的结构化的方式

SOA(Service oriented architecture)：对在不同业务领域，不同的系统，用统一的方式提供独立的服务

⑥XML 与 HTML 的设计区别是：XML 被设计为传输和存储数据，关注的是数据的内容。而 HTML 被设计用来显示数据，关注的是数据的外观。HTML 旨在显示信息，而 XML 旨在传输信息。

XM 和 HTML 语法区别：HTML 的标记不是所有的都需要成对出现，XML 则要求所有的标记必须成对出现；HTML 标记不区分大小写，XML 则大小敏感，即区分大小写。(XML 语法更严)

B.7 凭证管理系统

身份凭证和访问管理(ICAM)是结合数字身份和相关属性、凭证和访问控制的一个全面方法。国土安全部总统第 12 号令(HSPD-12)初步提供了一个通用的，标准化的身份凭证，使普通的物理访问证书安全并可互操作的在线交易。

现有的访问控制系统都升级过渡到“身份凭证和访问管理系统 ICAM”了。

C.整合身份即服务（如云身份）

整合身份服务 Integrating Identity Services/身份云服务

身份即服务，或身份和访问即为服务(IDaaS)，是一个第三方服务，SaaS 的一种，提供身份和访问管理。IDaaS 为云有效提供单点登录，并在内部客户访问那些基于云的软件即服务。谷歌、微软都提供 IDaaS，方便用户访问云资源。IDAAS 功能包括：

*身份管理：账号注册与维护。

*访问管理：用户认证，单点登录和强制授权。

*日志报告：行为记录。

它的功能角色就是实现更大的层次的安全策略，也主要实现管理企业的口令及其同步。

IDaaS 的典型案例：WidePoint Corp.

D. 整合第三方身份服务（例如：内部部署）

有 3 种方法来实施基于云的用户帐户管理,如 Office365 什么的软件：

①云的身份标识：在 Office 365 中用户创建和管理，并存储在 Windows Azure 活动目录(AD)。没有连接到任何其他目录。云身份没有集成的要求。每个用户在云中创建一次，账户只存在于 Windows Azure AD 中。

②目录同步：用户创建和管理有一个前提—身份提供者和 Windows Azure 的 AD 都是同步的，用于登录到 Office 365 目录同步使用现有的本地目录并同步到 Windows Azure AD。这种同步可以完成从一个本地活动目录使用目录同步工具，或从非 AD，本地目录使用 PowerShell 和 Azure AD 图形 API。同步意味着帐户被本地管理和属性不育街恿过 Office 365 云接口进行编辑。如果目录同步工具用于与 AD，那么口令散列也可以同步，因此用户可以在本地和云中使用相同的密码登录。

③统一身份/联合身份：除了目录同步，还对内部的身份提供登录处理请求。联合身份通常是用于实现单点登录。联合需要一个用户在使用联合身份时提供商对用户的密码进行检查。目录同步需要以填充基于云的目录作为一个先决条件。当使用联合身份时，许多 Office 365 的客户使用活动目录联合服务,其中管理登录密码检查在本地 Microsoft 活动目录基础设施。一些客户使用第三方身份提供商：微软支持 Office365 与各种资质合格的第三方身份提供商。

E. 实施和管理授权机制（授权机制的实现与管理）

一、怎么确定一个用户的访问权限？

有几种机制来实现：

1. 隐式拒绝 Implicit Deny

访问控制的基本原则是隐式拒绝，也就是默认拒绝，除非有授权。

2. 访问控制矩阵 Access Control Matrix

一个访问控制矩阵是一个包括主体、客体和分配权限的表格。其内容远远超过一个单一的访问控制列表(ACL)。

下面讲的功能表指定了某些主体对特定客体进行操作的访问权限。功能表和 ACL 完全不同，这是因为主体被绑定在功能表中（横的行），而客体被绑定在 ACL 中（竖的列）。

3. 功能表 Capability Tables

功能表是确定分配给主体特权的另一种方式。也不同于 ACL，因为功能表关注主体(如用户、组或角色)。例如，为会计角色创建的功能表将包括会计角色可以访问的所有客体列表，以及分配给会计角色对这些对象的特定权限。相比之下，ACL 专注于客体，会列出被授权访问文件的所高用户和/或组以及其具体授权内容的文件。

访问控制矩阵=功能表(行)+访问控制列表(列)；ACM=CT+ACL

4. 限制接口 Constrained Interface

如果用户没有权限去使用它，那么一个常见的方法是隐藏功能。例如，菜单命令不出现或者是灰色的、禁用的。

5. 基于内容的控制 Content-Dependent Control

数据库视图是基于内容的控制。一个视图从一个或多个表中的检索特定列，创建一个虚拟

表。被授子访问视图权的用户可以看到特定的数据字段，但不能访问底层表中的数据。

6.基于上下文的控制 Context-Dependent Control

在授予用户访问之前先审查用户之前特定的行为。例如，网上购物，如果购物车中的没有产品，就不可能进入支付功能；限制某资源的访问时间段也是这种机制。

7.需知/知其所需/知所必须 Need to Know

就算有机密级的授权，也不能所有机密都看，只能被授予看自己工作业务有关的内容。

8.最小特权 Least Privilege

主体只被授予他们完成工作职能时所需要的最小特权。和“需知”差不多，“特权”包括增、改、删什么的，“知”只包括查看。

9.职责分离 Separation of Duties and Responsibilities

关键数据、敏感功能必须分成由两个或两个以上员工来执行任务，这有助于通过创建一个制衡系统来防止共谋 Collusion、欺诈 Fraud 和错误。

CISSP 考试通常会在问题中拼出所有术语和缩略词，你不需要记住缩略词，不过最好还是熟悉下这些缩略语。

二、访问控制模型

就是指明主体如何访问客体的框架。通过访问控制技术和安全机制来加强模型的规则和目标。最常见有 3 种：自主、强制、角色，还有规则、非自主、基于属性也会考到。

E.1 基于角色的访问控制方法(R-BAC)

R-BAC 有助于通过防止特权蠕变(creep)，从而实施最小特权原则。特权蠕变是用户随着角色和访问需求的变化不断积累特权的过程和趋势。基于角色的访问控制在有频繁人事变动的动态环境中是有用的，因为管理员只需将新用户添加到适当的角色就可以轻松地授予多个权限。角色的访控主要是管主体的权限，而后面讲的自主访控主要是管客体的访问控制列表。与此类似的还有一种基于任务的访问控制模型：TBAC。

RBAC 提供两者职责分离（separations of duties）。

①静态职责分离 SSD（Static Separation of Duty (SSD) Relations through RBAC）：这种职责分离通过限制特权的联合（比如：用户不能是出纳和会计角色）来防止欺诈。

②动态职责分离 DSD（Dynamic Separation of Duties (DSD) Relations through RBAC）：这种职责分离通过限制可能在任何会话中启动的特权的联合（事实上：用户不能同时成为收银员和收银员监视者，但是用户可以是两个组的成员）来防止欺诈。

考题里会有一种混淆迷惑：

终端用户把某一个文件的访问权限分配给某一个用户组（如 Guest 组），这种方法不是基于角色，而是自主访控。因为最关键的要素是：基于角色的权限分配一定是由集中的授权者来实现的，也就是高级的系统管理员。只要是自己来分配，不管怎么分配，都是自主的访问控制。

RBAC 模型在具体软件中的实现方法有 2 种：：

①核心 RBAC

这个组件会集成到每一个 RBAC 实现中，其原因在于它是 RBAC 模型的基础。用户、角色、

权限、操作和会话应根据安全策略进行定义和对应。

- 用户和特权之间存在一种多对多关系。
- 会话是某个用户和一个已分配角色子集之间的对应关系。
- 提供传统但健壮的、基于组的访问控制。

许多用户可以属于多个组，并拥有每个组所享有的各种特权。当用户登入时(这是一个会话)，该用户所分配到的各种角色和组将立即对这名用户有效。如果你是 Accounting 角色、RD 组和 Administrative 角色的成员，那么你在登录后将立即拥有分配给这些组的所有权限。

因为在作出访问决策时能够包含其他组件，而不是仅仅根据一组凭证作出决策，所以这种模型提供了健壮的选择。RBAC 系统还可以配置为包含时间段、角色位置、星期几等。这意味着，除了用户 ID 和凭证之外，其他信息也可以用于访问决策。

②层次化 RBAC

这个组件允许管理员建立一个组织化 RBAC 模型，该模型对应特定环境中需要的组织机构和功能描述。因为各种业务已经建立在一个人员层次化结构中，所以该组件非常有用。很多时候，你在行政管理系统中的位置越高，你所拥有的访问权限就越多。

(1) 角色关系定义了用户成员和权限继承。例如，护士角色能够访问某些文件，实验室技术员角色则能够访问另外一些文件。医生角色继承了上述两个角色的权限和访问权利，而且还具有已经为医生角色分配的更多权限。因此，层次化是其他角色权限和权利的累积。

(2) 反映组织机构和功能描述。

(3) 存在两种层次类型：

- 有限层次只允许一个层次级别(角色 1 继承角色 2 的权限，并且没有继承其他角色)。
- 普通层次允许多个层次级别(角色 1 继承角色 2 和角色 3 的权限)。

层次是一种划分角色结构并反映组织机构授权和责任的自然方法。角色层次定义角色之间的继承关系。这种模型提供了两种不同的职责分离。（静态的 SSD 和动态的 DSD）

RBAC 实施控制的基本架构有 4 种：

①非 RBAC

非 RBAC 授予用户访问数据或通过传统的映射应用程序，如 ACL。这些没有正式的“角色”与映射关联，除了通过特定用户的任意标识。

②受限 RBAC

是当用户映射角色在单个应用程序，而不是通过组织范围的角色结构。在一个受限的 RBAC 系统的用户能够访问 non-RBAC-based 的应用程序或数据。受限 RBAC 的关键属性是用户的角色是在一个应用程序中定义的，而不是基于用户的组织工作的职能。

③混合 RBAC

基于用户在组织内特定的角色，适用于多个应用程序或系统。这角色然后应用于应用程序或系统，注册到组织的基于角色的模型。然而，随着“混合”一词表明，存在这样的情况，用户还可以被分配给仅在特定的应用程序定义的角色

④全 RBAC

是由组织的策略和访问控制的基础设施定义的角色控制，然后应用到整个企业的应用程序和系统。基于企业的应用程序，系统，以及相关的数据应用来定义权限，而不是一个特定的应

用程序或系统定义。

E.2 基于规则的访问控制方法(Rule-BAC)

一个基于规则的访问控制(Bule-BAC) Rule-based Access Controls，使用一套规则、限制或过滤器来确定能和不能出现在一个系统上的东西。它包括给予主体访问客体的权利，或授予主体执行一个动作的能力。有关规则-BAC 模型的一个独特特征是他们有适用于所有主体的全局规则。也就是说，它不区分用户，只看规则；不识别身份，只看行为。

规则-BAC 模型的最常见例子就是**防火墙**。防火墙包括 ACL 中的一组规则或过滤器，由管理员定义。防火墙都包含一个全局的、最终的规则(称为隐式拒绝规则)，会拒绝所有没有设定的流量（白名单）。

基于规则的访问控制还有另一实现方式：即基于属性的访问控制模型(ABAC) Attribute-based Access Controls。使用了属性比规则要更具体一些。许多**软件定义的网络**应用程序使用 ABAC 模型，可以定义不有的角色使用不同的网络服务。

E.3 强制访问控制（MAC）

强制访问控制（MAC）mandatory access control 模型，需要使用分类标签，并不使用规则。每个分类标签代表一个安全域或者安全领域。安全域是共享一个公共安全策略的主客体集合。也就是说，主体分为不同的密级，客体也分为不同的密级，同一密级的算是一个安全域。在桔皮书（通用准则 CC）里是等级 B。（前面基于规则的访问控制是不使用标签的），不过强制访控也算是基于规则的一种。

MAC 模型通常被称为**基于格子的模型** lattice-based model。MAC 模型是抑制型的、禁止性的，它基于隐式拒绝原则（implicit - deny philosophy），而不是直接拒绝原则（explicit - deny philosophy)。当然，同一密级的用户也要根据“知需”原则区分访问权限，同一密级的客体也要分成不同的组。不能什么都能看。这样，MAC 访问控制模型就有 3 种应用方式：

MAC 模型中的分类使用以下三种类型的环境之一（分层+隔离+混合）：

①分层环境 Hierarchical Environment

只区分密级来管理，高密级用户可以看低密级数据，低密级肯定不能访问高密级了。

②隔间区分环境 Compartmentalized Environment

不分密级，只按内容分隔间。每个域代表一个单独的隔间，有单独的权限管理。

②混合环境 Hybrid Environment

又分密级，又按内容分隔音。也就是客体管理的粒度更小了，不过管理起来也更麻烦。

这里插播一下“域”：

术语“域”早在 Microsoft 创办之前就已存在，CISSP 中多次出现“域”。然而，当人们听到这个术语时，他们通常想到的是网络区段中一组由一台运行 Microsoft 软件的服务器(称为域控制器)控制的计算机和设备。实际上一个域只是某个主体可用的一组资源。需要记住的是，主体可以是用户、进程或应用程序。在操作系统内部，每个进程都具有一个域，也就是该进程在执行自己的任务时可用的一组系统资源。这些资源可能是内存段、硬盘空间、操作系统

服务以及其他进程。在网络环境中，一个域是一组可用的物理和逻辑资源，包括路由器、文件服务器、FTP 服务、Web 服务器等。

术语“安全域”建立在域的基础之上，增加的内容只是这个逻辑结构(域)内的资源在相同安全策略下运行，并且由同一个组管理。因此，网络管理员可能会将所有的会计人员、计算机和网络资源放入域 1 中，而将所有的管理人员、计算机和网络资源放入域 2 中。这些项属于不同的容器，因为它们不仅实现相似的业务功能，而且更重要的是，它们具有相同的信任级别。正是这种共同的信任级别，才允许若干实体由单个安全策略管理。

不同的域由逻辑边界分隔，如防火墙、目录服务器等 。所有这些安全机制都是为每个域实施安全策略的组件。

域可以采用层次化结构，这种结构说明了不同域之间的关系以及不同域内主体的通信方式。主体能够访问相同或更低信任级别的域中的资源。它们的通信信道由安全代理(防火墙、路由器 ACL、目录服务)控制，不同的域则使用特定的子网掩码地址隔离。

需要记住的是，域不仅适用于网络设备和区段，而且还可以应用于用户和进程。

AIO 教材在关于单点登录的相关小节中谈到了域，这是因为，目前有几种不同的技术可用于定义和实施这些域以及与之对应的安全策略：Windows 环境中的域控制器、企业资源管理(ERM)产品、Microsoft Passport(现在的 Windows Live ID)以及提供 SSO 功能的各种产品。所有这些技术的目标是允许用户(主体)只需要登录一次就可以访问不同的域，而不必重新输入其他任何凭证。

E.4 自主访问控制(DAC)

1.自主访问控制(DAC) Discretionary Access Controls

由客体的所有者、创建者或一个客体的数据保管者来自行控制和定义主体对该客体的访问。常常使用客体的访问控制列表(ACL)来实现 DAC 模型。在桔皮书（通用准则 CC）里是等级 C。

自主访控有时也被称为基于身份的访问控制（identity - based access control model）。基于身份的访问控制是 DAC 的一个子集，因为系统识别用户身份并分配资源给这个身份。

2.非自主访问控制(NDAC) Nondiscretionary Access Controls

管理员对不可任意支配的访问控制进行集中管理。任何不是自主访问控制的模型都是非自主的。这包括基于规则、基于角色和基于格子的访问控制（前面都讲过）。

实际考题有问到哪个是非自主访问控制，答案一般都是基于角色的访问控制；如果问到非自主访问控制的模型特点，一般都是“通过中央授权来决定主体可以访问哪些客体”。

F.预防与减缓访问控制攻击

CISSP 里的经常讲到 mitigation，即 risk mitigation，翻译成风险**消减**最好。

一、骇客、黑客和攻击者

骇客、黑客和攻击者，Crackers, Hackers, and Attackers。

最早，骇客是干坏事的攻击者；黑客是不干坏事的技术高手；现在搞不清了，反正所有的攻击者被是黑客。现在就是“攻击者”来指代这些人。其它基础的知识就不说了，有关的攻击

技术和案例都很多了。

二、APT/高级持续性威胁 Advanced Persistent Threat

有国家或政府背景的，集团化的，高技术水平的，持续长期的网络空间作战威胁。CBK 里列举了塔吉特公司（Target）POS 机用户信用卡信息被窃的例子；其实 APT 最经典和轰动的案例是“震网”病毒。

三、针对访问控制的攻击

1.访问聚合攻击 Access Aggregation Attacks

通过收集多个非敏感信息块，并将他们结合来获得敏感信息。（第三域，E.3 章节里的数据库安全里，已经讲了聚合攻击和推理攻击）。网络侦察(Reconnaissance)就是是访问聚合攻击，结合多种工具来识别系统的多个元素，如 IP 地址、开放端口、运行服务、操作系统等等。

应结合严格访问控制、“需知”和最小特权原则来预防聚合攻击。

2.密码攻击 Password Attacks

破了管理员密码或特权密码，也就得到了一切。所以很多单位都要求必须设置“强密码”。

①字典攻击 Dictionary Attacks

密码攻击的一种，比暴力破解快此地，但必须要有好的字典。此外，字典式攻击经常会扫描差别构建式密码。一个差别构建式密码是之前使用过的密码，但有一个字符的不同。例如，password1 是 password 更改一个字符后的密码，其它的如 Password、lpassword 和 passXword 也是。攻击者在生成彩虹表时经常使用这种方法。

②暴力攻击 Brute-Force Attacks

密码攻击的一种，通过尝试所有可能的字母、数字和符号组合来发现用户帐户的密码。密码越长，计算量就越大。还有一种常用的方法是：散列值匹配查找。因为密码都不会在网络上发送，传输和存储的都是其散列值，所以只要能找到 1 个散列冲突（碰撞）collision，就可以实现登陆破解了。要破解散列值，就要用到生日悖论和彩虹表了。

③生日攻击 Birthday Attack

第三域 I.8 章节已经讲过生日悖论了。如果把 23 个人关在一个房间，那么任何两人同一天生日的可能性有 50%；如果有 367 人在一个房间里，你会有 100%的机会获得至少两个有相同生日的人。MD5 已经被破解了，SHA-3 目前还是安全的。

④彩虹表攻击 Rainbow Table Attacks

彩虹表预先计算好的各种字符串和散列值的映射数据库。使用 4 种字符类型的 14 位字符长度的密码的散列的彩虹表大约是 7.5GB 大小。这不大吧，可以大幅加快密码破解速度。

许多系统一般通过“加盐”密码来减少彩虹表攻击的有效性。盐是一组随机位，在散列前加到密码中。加密方法在散列前就加入附加位，这样随机性更大了，使攻击者更难以使用彩虹表密码

⑤嗅探攻击 Sniffer Attacks

一个嗅探器(也称为数据包分析器或协议分析仪)是)个软件应用程序，通过网络捕捉和分析流量。Wireshark 是一种受欢迎的协议分析器。

3.电子欺骗攻击 Spoofing Attacks/masquerading

电子欺骗(即伪装)是指假装成某物或某人等。电子欺骗的种类很多，有 IP 欺骗、邮件欺

骗、电话欺骗等等。

4.社会工程学攻击 Social Engineering Attacks

社会工程不难，但每次考试都会出几道题！社会工程就是与人斗，其乐无穷。

①网络钓鱼 Phishing

钓鱼邮件告知用户虚假信息，然后就能骗到有用的信息，或者实现木马植入。

②鱼叉式钓鱼 Spear Phishing

针对特定用户组的钓鱼方式。

③捕鲸 Whaling

捕鲸是的目标是大鱼、高层或高管。

④语音钓鱼 Vishing

纯属忽悠，就能搞定。

5.智能卡攻击 Smartcard Attacks

各种途径搞定卡的信息。

①故障生成(fault generation)攻击

攻击者通过操纵智能卡的一些环境组件(改变输入电压、时钟频率、温度波动)来引入这些“错误”。在向智能卡引入一个错误之后，攻击者会检查某个加密函数的结果，并查看没有出现错误时智能卡执行该函数得到的正确结果。分析这些不同的结果使得攻击者能够对加密过程进行反向工程，并有望获得加密密钥。这种攻击也称为故障生成攻击。

②旁路攻击(side-channel attack)

是非入侵式攻击，并且用于在不利用任何形式的缺陷或弱点的情况下找出与组件运作方式相关的敏感信息。针对智能卡的差分功率分析(differential power analysis，查看处理过程中的功率发射)、电磁分析(electromagnetic analysis. 查看发射出的频率)和计时(完成特定过程所需的时间)都是旁路攻击的示例。

③微区探查(microprobing)

使用针头和超声振动去除智能卡电路上的外部保护材料，随后就可以通过直接连接智能卡的 ROM 芯片来访问和操纵其中的数据。

6.拒绝服务攻击 Denial-of-Service Attacks

很普遍了，不解释。

7.网址嫁接 Pharming

是另一种类似的攻击，它将受害者重定向至一个看似合法的、其实仍是伪造的 Web 站点。

四、访问控制的安全防护方法汇总

1.物理上要保护好、隔离好服务器等核心设备。

2.加密、散列、加盐。

3.必须使用强密码。

4.输入时要隐藏密码（用*代替）。

5.必须使用多因素认证登陆。

6.使用帐户锁定技术防止暴力破解。

7.告知用户最后一次登陆的时间、地点。

8.安全意识培训。

G.管理身份与访问供给生命周期（如供给、审查）

身份信息和访问的开通、使用的生命周期包括：帐户的创建、管理和删除等 ，这些过程都很重要的，不然会出问题。这里讲账号的管理。

一、提供/开通/指派 Provisioning

一个新用户账户的初始创建通常被称为注册或登记。自己创建账号叫做 register；管理员创建账号叫做 Provisioning。没什么特别的内容。

二、审查/评审 Review

检查帐户以确保不活跃的账户被禁用以及员工没有过多的特权。要重点防范两个访问控制方面的问题：**特权过度**和**特权蠕变**。当用户拥有超过其工作任务所需的特权时就发生了特权过度；特权蠕变是指用户账户随工作角色和工作任务的改变而逐渐积累特权（因为不再需要的特权没有及时取消）。特权蠕变会导致特权过渡。

三、撤销 Revocation

无论员工以何种原因(包括休假)离开公司时，要及时**禁用**他们的用户账户。如果确定账户不再使用即可**注销**。一般情况下，账户禁用 30 天后会自动注销，这依公司需求而定。

第六域　安全评估与测试（设计、执行与分析安全测试）

Chapters 2,15,18 in OSG 7th

No Chapters in AIO 6th

A. 设计和验证评估与测试策略

一、基础知识

安全评估过程(程序)有三大主要活动：安全测试、安全评估和安全审计。

1. 安全测试 Security Testing（系统功能正常）内测

安全测试能够验证安全防护的控制措施在正常运行，包括自动扫描、工具辅助渗透测试和手动测试安全性。安全测试应该定期进行，需要关注保护组织机构的每个关键安全控件。

2. 安全评估 Security Assessments（综合能力达标）内测

安全评估是对系统、应用程序或其他测试环境的综合评价。在进行安全评估的过程中，受过培训的信息安全专家会执行风险评估以识别受测环境的漏洞，由此可根据需要做出折衷处理和提出修复建议。安全评估通常包括使用安全测试工具，但不只是自动扫描和手动渗透测试。他们还包括彻底审核威胁环境，当前和未来风险以及目标环境的价值。安全性评估的最终成果产品是一份用于管理的评估报告，这份报告以非技术性的语言描述了评估结果，并且以具体建议作为结论，从而提高被测环境的安全性。

3. 安全审计 Security Audits（安全管控有效）对外

安全审计会使用与安全评估期间相同的许多技术，但必须由独立的审计员执行。评估和测试结果仅供内部使用，旨在评估控制以求发现需要改进之处。从另一方面来说，审计就是评估，目的是向第三方展示控制的有效性。为机构设计、实施和监测控制的员工在评估这些控制有效性时存在固有的利益冲突。审计员对安全控件状态做出的评判应公正、无偏见。他们编写的报告与安全性评估报告非常类似，但这些报告的阅读对象不同，可能是机构的董事会、政府的监管人员和其他第三方。审计的类型主要有两种：内部审计和外部审计。

4. 漏洞评估/漏洞测试 Vulnerability Assessments

漏洞扫描和渗透测试为安全专家提供的视角是系统或应用技术控制的弱点。从术语角度更清晰的解释是，漏洞评估其实就是安全性测试工具，而非安全性评估工具。为保持语言的一致性，它们应该被称为漏洞测试。

二、有关角色

就 3 种角色是比较重要的，搞清楚它们的职能作用就行了。

1. 系统工程师和安全专家的角色

系统工程师和安全专家应当与赞助商共同来创建或论证测试和评估战略。他们可能被要要求提出用来管理风险的测试和评估方法，也可以监控测试和评估过程，如有需要，提出改进建议。他们也应当论证测试计划和流程。有时，他们会作为测试团队的顾问帮助指定相关的计划和流程。

2. 工作组的角色

一般情况下，企业需要抽组人员建立工作组来执行测试和评估战略。这个工作组常常被称为测试和评估集成产品小组，由测试和评估领域的专家，客户代表，和其他利益相关方组成。

3.验证 Verification 与确证 Validation

验证判断产品是否准确体现和满足了产品规范。（满足需求规格书）

确证是指软件或系统可以满足文档的需求和用户期望。（满足实际业务）

关于认证/认可什么的详细描述在第三域 C 章节的第 5 条。

B.执行安全控制测试

1.基于分类的 25 个最危险软件错误

2011 年 CWE/SANS（Common Wiakness Enumeration/SysAdmin,Audit,Network,Security）发布了 25 个最危险软件错误，即一个最广泛和关键的错误列表，这些错误可能导致严重的软件漏洞。它们常常很容易被发现和利用。它们之所以危险是因为黑客可以利用它们完全控制软件或使软件彻底不工作。CBK 里整理了三大高级类型的错误：

①组件之间不安全的交互,Insecure interaction between components（通信弱）

②高风险的资源管理,Risky resource management（管不好）

③漏洞百出的防御,porous defenses（防得差）

2.SANS 协会的关键安全控制

SANS 协会（SysAdmin audit Network Security），又叫系统管理和网络安全审计委员会，是提供计算机安全培训和专业认证的机构。除了上述 25 个最危险软件错误列表，SANS 关键安全控制列表是这一领域另一有价值的资源。特别是应用软件安全。其中第 6 号控制列表（CSC6）是为了管理所有内部开发或外部获取的软件安全生命周期而设计的，用来防止，探测和矫正安全弱点。具体列表就不复制了，在 CBK 里有。

B.1 脆弱性评估

一、脆弱性评估

目标：评估安全状态、查找全部漏洞、测试响应措施，测试前要告知可能的影响。

分类：

①黑盒测试，零了解，渗透团队在不了解测试目标的情况下测试。

②灰盒测试，中了解，在了解一些与测试目标相关的信息上测试。

③白盒测试，全了解，了解目标的本质的基础上测试。

评估内容还包括对员工的职能测试、社会学测试和对设备的物理性测试。评估结果仅针对当前时间，之后仍需定期评估。

为了做好脆弱性评估,安防人员最好在筹划准备阶段定义好具体的防护目标和要求,包括：

①威胁定义 threat definition;

②目标识别 target identification;

③系统(站点)特点 facility characteristics。

二、漏洞扫描 Vulnerability Scans

自动对系统、应用程序和网络进行探测，寻找可能会被攻击者利用的弱点。漏洞扫描的类型主要有三种：网络发现扫描、网络漏洞扫描和 Web 应用程序漏洞扫描。

1.网络发现扫描 Network Discovery Scanning

使用多种技术对一系列 IP 地址进行扫描，搜索配有开放网络端口的系统。网络发现扫描器实际上不能探测系统的漏洞，只是提供一份网络检测的系统显示报告和一份端口清单，这份清单通过网络和服务器防火墙公开了隐藏在扫描器和扫描系统之间网络路径中的端口。

①TCP-SYN 扫描。“半开放”扫描，向每个被扫描的端口发送带有 SYN 标志设置的单个数据包，也就是请求一个新连接。如果扫描器收到了 SYN 和 ACK 标志设置的响应包，则表明该且端口是开放的，TCP 握手移至第二阶段。

②TCP 连接扫描。向指定端口的远程系统打开一个全连接。这种扫描的使用情景是，扫描用户没有运行“半开放”扫描的必要权限。

③TCP-ACK 扫描。发送带有 ACK 标志设置的单个数据包，表明它是开放连接的一部分。

④Xmas 扫描。发送带有 FIN 、PSH 和 URG 标志设置的数据包。这个数据包带有很多标志设置，被称为是“点亮的圣诞树” Christmas tree，从而给这种扫描起了这个名字。

TCP 的三次握手和详细知识看第四域的 A.1 章节。

⑤扫描神器 NMAP

解释一下 NMAP 扫描结果的三种端口状态：

*开放/在用 open：端口在远程系统上是开放的，有一个应用程序正在连接该端口。

*关闭/未用 closed：端口在远程系统上可用，防火墙允许通，但无应用程序连接该端口。

*过滤/阻拦/未知 filtered：无法确定状态，很可能防火墙过滤了。

2.网络漏洞扫描 Network Vulnerability Scanning

网络漏洞扫描在检测到开放端口后会继续调查目标系统或网络，来查找已知的漏洞。在某些情况下，扫描器可能没有足够的信息来最终确定一个漏洞的存在，它也可能会在没有问题的时候报告漏洞，这种情况被称为**假性正面**报告 false positive report（**误报**）。更危险的是，漏洞扫描器可能会漏掉漏洞，从而不能提醒管理员危险情况的存在，这个错误被称为**假性负面**报告 false negative report（**漏报**）。

3.Web 漏洞扫描 Web Vulnerability Scanning

Web 服务器上的应用程序是复杂的，经常对底层数据库有访问特权。攻击者通常使用 SQL 注入和其他针对 Web 应用程序的安全设计缺陷来攻击。

B.2 渗透测试

渗透测试 PT（Penetration Testing）超越了漏洞测试技术。渗透，就是攻击成功了，入侵者能够突破系统环境的边界。安全的一个重要目标就是防止渗透。因为它不止是找出漏洞，更要利用漏洞进行模拟攻击。渗透测试人员通常使用一个工具叫 Metasploit，还有 KALI 也用得很多。有人把渗透测试等同与安全评估，其实安全评估的范围大得多，不只是网络渗透，还有物理安全、人员安全、管理安全什么的。

根据双方的关系，分为盲测、双盲测、目标测试。

根据掌握的信息，分为零知识（黑盒）、部分知识（灰盒）、全知识（白盒）。

白盒有 2 种英文：Crystal box（水晶盒）、white box。

黑盒也有另一种说法：realistic type of penetration test（基于现实的测试）

考试里的渗透测试步骤是这样的：

①discovery 发现，搜集和收集目标的相关信息

②enumeration 枚举，进行端口扫描和资源标识方法

③vulnerability mapping 脆弱性映射，在确定的系统和资源中标识脆弱性

④exploitation 利用，尝试利用脆弱性进行未授权访问

⑤report to manager 向管理层报告，向管理层提交报告和安全建议

（搜、举、射、用、报）

脆弱性评估（测试）与渗透测试的区别：

前者扫描环境中存在的所有可能漏洞；后者找出并利用漏洞入侵客户系统。

选择一个安全测试或渗透测试采用的方法/工具，应考虑以下因素：

①攻击面 Attack Surface。用不同的工具查找不同类型的漏洞。

②应用类型 Application type。对不同的软件系统用不同的测试方法。

③测试结果的质量要求和用途 Quality of Results and Usability。不同标准（低误报、零漏报）、不同用途（如评标、主级等）对应不同的方法。

④功能特点 Supported Technologies。评测工具有自身的功能特点，有的只管 C 语言，有的只能搞网站。

⑤性能要求 Performance and Resource Utilization。不同的工具需要不同的计算能力、人力、经费等。

考试中经常涉及的渗透测试的工具：

①Nikto/Burp Suite/Wapiti：web 服务、web 应用的漏洞扫描。

②Metasploit：渗透测试工具集，包括网络扫描、漏洞扫描等，并不针对某一特定功能。

③sqlmap：SQL 注入测试。

④Nmap：端口扫描神器。

⑤Nessus：漏洞扫描。

安全内容自动操作协议 SCAP(The Security Content Automation Protocol)，是用来处理漏洞信息和漏洞管理信息的通信规范，可以传输和保护漏洞信息和安全配置信息(CVE、NVD)。

通用漏洞评级系统 CVSS(Common Vulnerability Scoring System)，是用来称量和量化漏洞的风险等级、影响程度的指标，也包括了消减建议等内容。

NVD(National Vulnerability Database),国家漏洞库。

CVE(Common Vulnerabilities and Exposures),通用公共漏洞库和暴露。

CSV(Comma-Separated Values)不知道是什么。

B.3 日志审查

信息安全管理人员应该定期进行日志审查，以确保特权用户不滥用特权。安全信息和事件管理(SIEM)系统在这些过程中发挥重要作用，将日志审查的大部分日常工作自动化。

1.日志

日志是系统和网络中发生的事件记录。日志由一些日志项组成，每个日志项包含了与系统和网络中发生的事件相关的信息。安全日志有很多源头，比如安全软件(反病毒软件，防火墙，

入侵探测和防御系统），工作站和服务器的操作系统，网络设备和应用软件等。

2.日志管理

安全日志管理：生成，传输，存储，分析，和废弃计算机安全日志数据的全过程。

3.日志分析

网络和系统管理员传统上负责执行日志分析——研究日志记录以辨识感兴趣的事件。

4.日志的作用

①进行审计和取证调查；②内部调查；③建立基线；④识别运行趋势以及发现长期问题。

5.最常见的与安全相关的操作系统数据

①系统事件：系统事件就是由操作系统组件执行的操作行动，比如关机，启动服务等。一般来说失败的事件和最重要的成功事件应当被记录，但是大多数操作系统允许管理员指定哪类事件需要被记录在日志里。每个事件被记录的细节也大相径庭：每个事件一般有时间戳，以及其他信息，比如事件状态，错误码，服务名和事件有关的用户或系统账号。

②审计记录：审计记录包含安全事件信息比如成功和失败的身份认证尝试，文件访问，安全策略变更，账号变更(账号创建，删除，账号权限分配)，以及权限的使用。操作系统通常允许系统管理员指定哪些类型的事件应被审计以及是否记录执行特定活动的成功或失败的尝试信息。

B.4 综合事务/综合交易/合成交易 synthetic transactions

搞信息系统运行维护的一项重要任务就是监控掌握各类事务（业务）的运行状态，包括人工检测和自动检测。

1.实际用户监控(RUM)（考点）

实际用户监控(RUM)/真实用户监控，是 Web 监控的一种方式，旨在捕获和分析网站或应用的**每个用户的每个交易**。有时也被称为实际用户测量，实际用户度量，或终端用户体验监控(RUM)，是一种被动监控方式，依赖于可以持续观察系统行为，追踪可用性，功能性和反应时间的 Web 监控服务。人工的性能监控，也被称为被动监控，使用轻量级的、低水平的代理来完成，如 JavvaScript,CSS,和 AJAX 的调用等。

一些**自下而上** bottom-up forms 的实际用户监控(RUM)依赖于捕获服务器侧信息，以重建用户体验，而**自上而下** top-down client side 的基于客户端的实际用户监控(RUM)则可以直接看到用户如何与应用交互，以及他们的体验究竟如何。（下是服务器）

2.人工合成交易/综合交易的性能监控/综合性能监控/合成性能监控 synthetic transactions

监控真实的用户要追踪实际用户的会话，容易出现躁音（误差）；更有效的是使用自动工具模拟一个脚本化的浏览器进行集成测试，它能精确测量在线时间，获取更多的功能和性能细节，并提供图形化的态势界面。其实就是一套综合的性能管控系统。综合交易也有翻译成：人工合成交易的。它不跟踪用户实际的会话。

使用综合交易监控的典型例子是：微软的系统中心运行管理器。使用它你能够创造不同类型的合成交易，用于监控数据库、网站和 TCP 端口的使用。

监控的方式通常有：①监控 Web **站点**；②监控**数据库**；③监控 TCP **端口**。

B.5 代码审核与测试 （例如：手动、 动态、静态、 模糊测试）

第八域 C.3 章节也讲了软件的测试，什么白盒测试（代码）、黑盒测试（功能）、统计测试、变更测试、单元测试、集成测试、系统测试就不在这讲了，都很容易理解。（这是考点）

软件开发时的安全脆弱性的起因有很多（考点），如：

①不良编程习惯；Bad programming patterns（习惯差）

②安全基础设施的错误配置；Misconfiguration of security infrastructures（配置错）

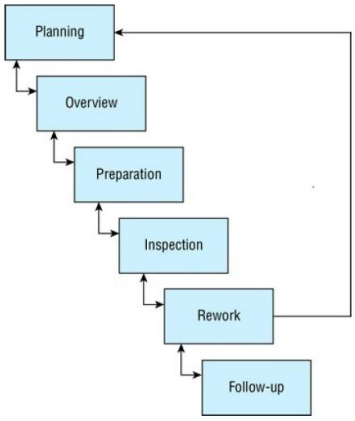
③安全基础设施的功能缺陷；Functional bugs in security infrastructures（功能弱）

④实施过程中存在逻辑缺陷。Logical flaws in the implemented processes（逻辑乱）

缺陷不是漏洞。

1.代码审查（Code Review）

是软件评估程序的基础。在代码审查(也称为“并行审核”peer review)期间，由不是写代码的开发人员进行审查、查找缺陷。最正式的代码评审过程，称为范根检查法 Fagan inspections 或 Fagan testing，有六个步骤：



①规划 Planning

②概述 Overview

③准备 Preparation

④检查 Inspection

⑤返工 Rework

⑥后续 Follow-up

2.静态测试 Static Testing

在不运行软件的情况下通过分析源代码或编译的应用程序对软件进行评估。静态分析通常涉及用来检测常见软件缺陷(如缓冲区溢出)的自动化工具。在成熟的开发环境中，应用程序开发人员能够使用静态分析工具，并在设计、开发和测试过程中使用它们。

3.动态测试 Dynamic Testing

动态测试是在运行环境中评估软件安全，对于部署别人写的应用程序的组织来说通常是唯一选择。在这种情况下，测试人员经常不能访问底层的源代码。动态软件测试的一个常见的例子是使用 Web 应用程序扫描工具来检测 Web 应用程序中跨站点脚本、SQL 注入或其他缺陷的存在。对生产环境的动态测试应该小心谨慎，以避免服务意外中断。

动态测试也可以使用综合事务/合成交易（synthetic transactions）来验证系统的性能。

4.Fuzzing（模糊测试）Fuzz Testing（考点）

模糊测试是黑盒测试，有点像误用例测试，就是随意乱输入数据来测试软件的功能和性能。是一项专门的动态测试技术，它向软件提供了许多不同类型的输入，来强调其局限性并发现先前未被发现的缺陷。模糊测试软件向软件提供无效的输入，或者是随机生成，或者是特别制作以触发特殊的软件漏洞。然后，模糊测试监控应用程序的性能，监视软件崩溃、缓冲区溢出或其他不良和/或不可预知的结果。

有两种方法：

①变异（修改），Mutation (Dumb) Fuzzing。修改下实际运行的数据来测试。

②智能（生成），Generational (Intelligent) Fuzzing。这个难搞，要基于对程序所使用数据类型的理解，开发新的数据模型并创建新的模糊输入。

模糊测试常用的工具软件是 zzuf！

5. 软件测试和代码测试

一旦代码检查成功结束，软件测试就开始了。先从单元级别测试开始，最后做系统级别测试。有时可能还有一个集成级别的测试。

B.6 误用例测试

在软件测试中有两个主要的测试战略：正面测试和负面测试

①正面测试/正向测试 Positive Testing，确定你的应用按预期工作，如果在测试中发现一个错误，则测试失败。

②负面测试/负向测试 Nagative Testing，确保你的应用能够很好地处理无效输入或非预期的用户行为。

用例是对于系统及其环境之间交互的抽象场景（程序员都懂）。一个用例定义了系统和环境可能发生交互时共享的系统或对话的方式。一个场景描述了在特定个人之间的特定交互。用例把同类系统和使用系统的行动方之间交互的示例性场景加以抽象。

误用例 misuse case，也有称为“滥用用例”，就是人为的做一个错误的行为，去测试软件的应对能力。软件测试人员使用一个称为误用案例测试或滥用用例测试的过程来评估他们的软件对这些已知风险的脆弱性。在误用用例测试中，测试人员首先列举已知的误用用例。然后他们试图使用手动和/或自动攻击技术开发这些用例。

关于详细的测试分类，见第八域 C.3 章节。

B.7 测试覆盖率分析（度量标准）

结构化测试的水平可以使用设计好的度量标准来评估。一般来说使用在结构化测试中软件结构完成评估的百分比来表示。这些度量标准一般称为“覆盖”，是针对测试选择准则测量其完成度。结构化覆盖的完成数量应当与软件所面临的风险水平相对应。使用“覆盖”这一术语通常意味着 100%覆盖。比如，如果一个测试程序已经实现“语句覆盖”，这意味着软件中 100%的语句已经被至少执行了一次。题目中问 statement coverage，别理解错了，它应该翻译成语句覆盖。

常见的结构化覆盖（structured coverage）：

①语句覆盖 statement coverage：这一准则要求每个程序语句至少执行一次测试，并为此提供充足的测试用例；但是实现语句覆盖不能为软件产品的行为提供充足的信心。

②决策/判断(分支)覆盖 decision(branch) coverage：这一准则要求每个程序决策或分支被执行，并为此提供充足的测试用例，以使每个可能的输出至少出现一次。对多数软件产品来说，这被认为是最低水平的覆盖。但是仅仅是决策覆盖对于高完整性应用来说是不够的。

③条件覆盖 condition coverage：这一准则要求程序决策的每个条件所呈现的所有可能的输出必须至少执行一次测试，并为此提供充足的测试用例。只有当必须评估多条件以达到决策时，条件覆盖才与分支覆盖有所不同。

④多条件覆盖 multi-condition coverage：这一准则要求在一个程序决策的所有组合条件执行测试，并为此提供充足的测试用例。

⑤循环覆盖 loop coverage：这一准则要求所有程序被循环执行，从 0,1,2 以至于多次重复，覆盖启动，典型运行，和中止(边界)条件。

⑥路径覆盖 path coverage：这一准则要求每个可能的路径，基础路径等，从程序代码段的入口到出口，至少执行一次测试，并为此提供充足的测试用例。由于在软件程序中存在大量可能的路径，路径覆盖一般很难实现。一般根据被测软件的风险大小和关键程度，确定路径覆盖的数量。

⑦数据流覆盖 data flow coverage：这一准则要求每个可能的数据流至少执行一次测试，并为此提供充足的测试用例。目前有一些可用的数据流测试战略。

B.8 接口测试 （例如： API，UI，物理）

接口测试（Interface Testing）是开发复杂软件系统的一个重要组成部分。被分别开发的模块之间的数据传递使用定义良好的接口，以便团队可以独立工作；接口测试就是评估模块接口的性能，以确保所有开发工作完成后模块会正常工作。有三种接口要进行测试：

①应用程序编程接口(API) Application Programming Interfaces

测试模块的数据交互。

②用户界面(UI) User Interfaces

包括图形用户界面(GUI)graphical user interfaces 和命令行接口(CLI)command-line interfaces，要审查所有的用户界面是否能正常运作。考题会列出一个命令行的测试，答案一般都是“接口测试”，别错选了 API 测试。

③**物理**接口 Physical Interfaces

其它的物理接口。

C.收集安全流程数据（例如： 管理和运营控制措施）

1.信息安全持续监控 Information security continuous monitoring（ISCM）（考点）

用于支持企业的信息安全风险决策；确保安全策略有效实施；保持对信息安全、脆弱性和威胁的持续了解，为组织的风险管理决策提供支撑。做好监控需要预先定义好各项测量指标 Metrics，如漏洞的数量与严重程度、尝试非法访问的次数、风险容忍的阈值等等。

2.ISCM 开发过程

①制定 ISCM 战略；Define

②建立 ISCM 程序；establish

③实施 ISCM 程序；implement

④收集安全相关信息；（考题中有的没这步）

⑤分析收集到的信息并形成结果报告；analyze and report

⑥对这些结果作出响应；respond

⑦回顾并更新监控程序。Review and update（考题中有的把这步拆分成 2 步了）

3.度量标准/监控频率

根据 NIST SP 800-137，对于联邦信息系统和组织的信息安全持续监控(ISCM)，安全实践者需要在确定度量系统的监控频率或安全控制的评估频率时，把下列准则考虑在内：

①安全控制的易变性：易变的安全控制应被更频繁地评估，无论评估目的在于确定安全控制的有效性还是支持对度量指标的计算。

②系统分类/影响水平：一般来说，分类为高影响度系统的安全控制要比中、低影响度的系统上被更频繁地监控。

③提供关键功能的安全控制或特走评估目标：提供关键功能的安全控制或特定评估目标(比如日志管理服务器，防火墙)应当更频繁地被监控。另外，支持关键安全功能的个别评估目标被认为是对系统很关键的(根据业务影响分析)。

④对于已经辨识的弱点的安全控制：一般认为，已经记录在安全评估报告(SARs)的现存风险需要更频繁地监控以确保风险在可容忍范围内。

⑤组织风险容忍水平：对风险容忍水平低的组织(比如处理，存储，或传输大量专有和/或个人身份识别信息的组织，有大量高等级系统的组织，面临特定持续性威胁的组织）会比对风险容忍水平高的组织(比如拥有大量中低等级的系统，基本不处理，存储或传输专有的/或个人身份识别信息的组织)更频繁地监控安全态势。

⑥威胁信息：组织要考虑现有可信的威胁信息，包括已知的漏洞，攻击场景。

⑦薄弱点信息：在决定监控频率时，组织要考虑与信息技术产品相关的最新薄弱点信息。比如，如果一个特定产品厂商每月提供软件补丁，组织就可以考虑至少每月一次执行漏洞扫描。

⑧风险评估结果：检查组织的、或系统的风险评估结果，并在决定监控频率时考虑这些结果的影响。如果在组织内部有风险打分系统，风险的分值可能被用来证明增加或减少对相关控制的监控频率的合理性。

⑨报告要求：报告要求不会驱动 ISCM 战略，但是可能对监控频率产生影响。比如如果组织策略要求每个季度报告非授权组件数量和采取的纠正性行动，组织将至少每季度监控系统以发现非授权组件。

C.1 账户管理 （例如：升级、撤销）

在第五域的 G 章节也讲到身份信息的管理了，即身份信息和访问的开通、使用的生命周期包括：帐户的创建、管理和删除等，这些过程都很重要的，不然会出问题。它和账户管理还是有区别的。

1.身份信息管理

①提供/开通/指派 Provisioning：一个新用户账户的初始创建，称为注册或登记。

②审查/评审 Review：检查帐户以确保不活跃的账户被禁用以及员工没有过多的特权。

③撤销 Revocation：无论员工以何种原因离开公司，要及时禁用他们的用户账户。

2.账户管理

①增加账户。首先用户要悉知并接受系统使用政策，然后还有账号期限、口令强度等要求。

②修改账户。特权账号要严控，尽量少用、不用，别滥用。

③停用账户。人走茶凉。

C.2 管理评审 management reviews

管理评审是对管理进行评审，公司**高管召开会议**来研究管理机制是是否完全达到公司要求、符合公司目标。

C.3 关键绩效与风险指标

这是两个最重要的信息安全度量标准，即 KPIs（key performance indicators）和 KRIs（key risk Indicators），关键性能指标和关键风险指标。ISO 27004 给出了衡量安全管控效能的标准。

KPI 是评估所有关键业务功能是否有效运行的指标，即系统运维关注的运行**质量状况**；

KRI 是展现某些特殊操作是否带来安全风险的指标，即安全监察关注的所有**风险变化**。

C.4 验证备份数据

数据必须有效备份，并能按需恢复。用户数据、数据库、邮件等要用不同级别的备份策略。

C.5 培训与意识

培训是提高技能，意识是提高警惕。社会工程通过搞定人的因素而轻易得到相关信息或资产，典型的社会工程应用方式就是钓鱼（phishing），其中精确指向的钓鱼(spear phishing)专门针对高官、高管人群，也称为捕鲸（whaling）。此外，借口套话（pretexting）方式常用来骗取对方的账号信息。

C.6 灾难恢复与业务连续性

业务持续计划（BCP）以及灾难恢复计划（DRP）应定期评测并修订。

第一域 G 章节，第七域 M、N 章节都讲了 BCP，都要掌握。

D. 分析与报告测试结果（例如：自动、手动）

写报告是最烦人的事，也是最需要综合素质的事，工作量很大，在熟悉技术方案、掌握测试情况的基础上，必须按照管理层的需求，以商业运营的角度去客观、生动、浅易地描述安全状况。技术报告不是对扫描结果的简单罗列，要从分析模型方法、分析测试结果、量化风险影响、提出对策措施、核算成本收益等多个方面进行研究，最终给出精准可行的报告，为管理层提供辅助决策支持。

E. 开展或促进内部和第三方审计

美国联邦信息安全法案（FISMA Federal Information Security Management Act）要求联邦机构**每年**至少对组织的信息安全体系进行一次自我审计和独立的第三方审计。信息安全专家需要理解法律标准，虽然完全做到很难，但必须确保有恰当的范围和合理的目标用于相应的安全级别，并实施合理的控制。

内部审计与外部审计各自有优缺点：**内部审计**的人员对公司情况更熟悉，协调公司内部资源更顺畅，且对外暴露公司资产的风险较小，但也存在内部关系复杂，人为隐蔽、瞒报问题的

情况。**外部审计**往往有更多其它系统安全测试的经验，且由于不了解公司、不受利益制约，可以更客观更彻底的随意查找并暴露问题，但耗时较长，外部审计的收费还很昂贵，且必须受监管以避免内部信息泄露。

1.有关审计标准的陈述(SAS)70

历史上，许多组织常借鉴 Statement on Auditing Standards (SAS) 70 reports 审计准则来有效管控外包服务，然而 SAS 70 关注财务报告内部控制(ICOFR)specifically on risks related to internal control over financial reporting，并不关注系统可用性和安全。SAS 70 报告已在 2011 退休，取代财务报告内部控制(ICOFR)的是：服务组织控制报告 **SOC**（Service Organization Control)报告。在过去，SAS 70 报告的目的是辅助做财务报表审计。现在三个类型的 SOC 报告已经被定义以取代 SAS 70 报告并解决更广泛的特定用户需求一比如解决安全，隐私，和可用性问题。另外，服务组织正在寻找更好的方式以提供对于它们控制环境的保障。

2.SOC 报告类型（Service Organization Control(SOC) reports）（必考）

服务组织控制报告/SOC 报告，通常覆盖过去 **12 个月**有关设计和控制有效性的活动，每年都要持续报告以满足财务管理或安全治理要求。在有些场合，一个 SOC 报告也可能覆盖一个较短的时间段，比如六个月，或特定时间点，一般用于新系统/服务的控制设计或者对于系统/服务的最初检查(审计)。（SOC 共有 3 种 2 类）

①SOC1 报告：仅关于财务的审计报告。

②SOC2 报告：详细的专业的安全服务审计报告（可用、机密、完整性，隐私什么的）。

③SOC3 报告：简要的公开的安全服务审计报告（可用、机密、完整性，隐私什么的）。

一类/Ⅰ类报告：提供针对某个时间**点**的审计报告。（Ⅰ是点，Ⅱ是段）

二类/Ⅱ类报告：提供针对一个时间**段**的审计报告。（新系统、新服务什么的）

比如，如果一个组织需要覆盖特定系统的安全与可用性的时间段报告，组织将要求服务提供商给予 SOC 2 的Ⅱ类安全与可用性报告。如果组织需要覆盖财务报告内部控制(ICOFR)的时间点报告，组织将要求服务提供商给予 SOC 1 的Ⅰ类报告。

SOC2 要求每 6 个月发布 1 次。审计的流程、阶段都很简单，不说了。

3.SSAE-16

从 2011 年 6 月开始，SSAE 16 正式替代了 SAS 70。即指美国注册会计师协会(AICPA)制定的-**鉴证业务准则公告第 16 号**（Statements on Standards for Attestation Engagements No.16，简称 SSAE 16）。这一准则要求企业遵循 **ISAE 3402**《鉴证业务国际准则第 3402 号》（International Standards for Assurance Engagements ISAE-No.3402）中规定的国际服务组织报告准则。SSAE 16 认证和 ISAE 3402 合规都要求一名独立审计师对服务组织的内部控制进行严格审查。

第七域　安全运营（例如：基础概念、调查、事件管理、灾难恢复）

Chapters 3,10,16,17,18,19 in OSG 7th

Chapters 5,8,9,11 in AIO 6th

A.理解与支持调理/知道什么是调查取证

信息安全是直接关系到公司资产和利益的事，美国是法治社会，所以讲运营一上来就先搞法律法规的东西，就是组织必须实施和证明其合法、合规、合道德，并利用法律指控坏人。为了搞到证据或者得到日志告警什么的，就有一系列的针对攻击的安全方面的运营工作要做了。

A.1 证据采集与处理 （例如： 监管链、 访谈）

罗卡交换定律（Locard’s Exchange Principle）指出，在犯罪现场中，罪犯拿走了多少东西，那么就会相应的留下多少东西。这一原则同样适用于纯数字的犯罪现场，使我们能够找出相关的责任人。

计算机犯罪类似于传统的犯罪，必须理解 MOM——动机、机会和手段（Motive,Oportunity, And Means），计算机犯罪也具有特定的惯用手法(Modus Operandi, MO [method of operation])。了解罪犯的 MO 与签名行为对整个调查过程都十分有用，可以用来识别相同罪犯的其他攻击，也可以提供在会谈、讯问和审判过程中非常有用的信息，还可以引导控制心理犯罪情景分析(定形)。定形提供了对攻击者思考过程的洞察，并且可以用于标识攻击者。

数据调查有很多不同的名字：计算机取证（computer forensics）、数字取证（digital forensics ）和网络取证(network forensics)到电子数据发现（electronic data discovery）、电脑网络取证（cyber forensics）和取证计算（forensics computer）等等。

1.现行法律主要针对 3 种类型的计算机犯罪（cyber law）：

计算机辅助犯罪(computer-assistedcrime)是指用计算机作为工具来帮助实施传统犯罪。

针对计算机的犯罪(computer-targeted crime)是指计算机系统成为被攻击的受害者。

计算机牵涉型攻击(computer is incidental)是指计算机不一定是攻击者或被攻击者，只是在攻击发生时碰巧涉及其中。

通常，许多受到伤害的公司只希望确保攻击者利用的脆弱性得到修复，而不愿花时间和金钱来追捕与起诉攻击者，这是使得网络罪犯逍遥法外的主要原因。

2.可接纳的证据 Admissible Evidence

CBK 里的描述是，证据必须满足 5 个条件(五项证据规则)(真、准、全、信服、接)：

①真实 be authentic。证据必须是来源于真实场景、并符合当时的真实场景。

②准确 be accurate。收集、使用过程必须保持证据的准确、无误。

③全面/完全 be complete。所有相关的证据都要收集，确保其全面、可靠、无遗漏。

④有说服力 be convincing。证据应该清楚、明晰和容易理解，对陪审团来说是可信的。

⑤可被接纳 be admissible。证据必须合规，能够在法庭上使用，能够证明重要事实。For evidence to be admissible, it must be relevant, complete, sufficient, and reliable to the case.这最后一条 admissible，在官方学习指南（OSG）里的描述是，在法庭上采纳的

证据必须满足3个基本要求(想必发)：

1)相关性。证据必须能证明某个确定事实。

2)必要性。证据必须对本案是必要的，起关键作用的。

3)合法性。证据必须合法获得。

3.证据链/监管链/保管链 Chain of Evidence

在法庭上,仅通过证人来证明某物品的归属是不严谨、不可靠的。还必须建立证据链（chain of evidence），也被称为证据保管链或监管链（chain of custody），包括所有处理证据的人，包括收集的警员、处理的技术人员以及律师等等，证据必须有全寿命的完整记录，以确保是同一证据，处理证据的每个人都必须签署监管日志链（证据履历表），以提供完整的事件序列，从而说明从证据收集开始到审问之间的过程。

4.证据的类型 Types of Evidence

在法庭上可用的证据有3种类型：

①实物证据 Real Evidence

实物证据也被称为客观证据（object evidence），包括那些可能会被实际带到法庭上的物品。如凶器、衣物、键盘、硬盘等。

②文档证据/书面证明 Documentary Evidence

文档证据包括所有带到法庭上证明事实的书面内容。如系统日志等。

使用文档证据，除了“想必发”3个基本要求外，还必须遵从2项基本规则：

一是最佳证据规则 best evidence rule（复印无效）。当文档作为法庭处理的证据时，必须提供原始文档，复印件没有法律效应。

二是口头证据规则 parol evidence rule（口说无凭）。当双方的协议被以书面的形式记载下来时，一切口头协议都是无效的，只认书面。

③言词证据/供述陈词 Testimonial Evidence

言词证据十分简单，就是证词的证据，证词既可以是法庭上的口头证词，也可以是记录存储的书面证词。

有很多关于证据的原则和合法规则经常考到，实在搞球不清楚，不翻译了。

5.犯罪调查的三要素：

①情报，Information accumulation 信息累积：是调查的基本要素。

②工具，Instrumentation：工具在调查财务等相关犯罪时，要用的扫描、采集等各类计算机系统和其它工具软件和设备。

③访谈，Interviewing：深入了解动机想办法套话，尤其对内部人员。

（望闻、问、切）

6.访谈/采访/录口供

没什么好说的。

7.电子取证原则

数字证据科学工作组(SWGDE)是一个国际组织，它设计的通用准则被用于8国集团（G8）作为计算机取证和数字/电子取证的6大原则（A.3章节又重复强调了一遍）：

①合规性。处理数字证据时，必须遵循所有通用取证的程序原则。

②完整性。查封数字证据时，所采取的行动不得改变证据。

③有能力。访问原始数字时，该人必须受过专门培训。

④可审计。保管数字证据时，扣、访、存或传等所有活动，必须被记录，以供审查。

⑤可问责。某人拥有证据时，要对其一切操作行为负责。

⑥通用性。任何的组织机构，扣、访、存或传证据必须合规，并承担责任。

8.证物磁盘管理员的 4 大职责 forensic disk Controller performs 4 functions

①写保护、防篡改。Write blocking, intercepts write commands sent to the device and prevents them from modifying data on the device.

②取数据。returning data requested by a read operation。

③查访问日志。returning access-significant information from the device。

④报情况给取证专家。reporting errors from the device back to the forensic host.

A.2 报告与记录

如果一个事件响应小组怀疑事件已经发生，他们应该开始记录有关该事件的信息。任何和事件有关的信息应该被记录并带有时间戳。所有的文件应当注明日期并由调查人员签名。事件响应团队一直需要注意对于任何范围的数据或系统被调查，应该使用适当的采集技术，正如上面讨论的。

搞通信运维或网络管理的都知道，机房台站的值勤值班都必须要做好表报资料的登统计（这就是记录）；还必须及时请示上报重要情况（这就是报告）。

A.3 调查技术 （例如：根本原因分析、事件处理）

1.计算机犯罪的主要类别 Major Categories of Computer Crime

计算机犯罪是与计算机相关的违反法律或法规的犯罪行为，通常分为 6 类：

①军事和情报攻击 Military and Intelligence Attacks（国安）

军事和情报攻击主要用于从执法机关或军事和技术研究机构获得秘密和受限的信息。这些信息的暴露可能使研究泄密、中断军事计划甚至威胁国家安金。收集军事信息或其他敏感信息的攻击常常是其他更具破坏性攻击的前兆。在“震网”事件后，网络空间作战更加意义重大了，而且形成了“高级持续性威胁”（ATP 攻击）Advanced Persistent Threats。攻击者拥有资金，并拥有先进的技术技能和资源。他们代表一个民族国家、犯罪组织，恐怖组织，或其他发起人，对一个非常集中的目标进行持续有效的攻击。

②商业攻击 Business Attacks（窃密）

商业攻击专门非法获取公司的机密信息。对竞争者机密信息的收集也称做工业间谍活动。

③财务攻击 Financial Attacks（偷钱）

财务攻击被用于非法获得钱财和服务。财务攻击的目标可能会是增加银行账户中的存款，或者是免费打长途电话。

④恐怖攻击 Terrorist Attacks（暴乱）

恐怖攻击实际上存在于我们这个社会的很多领域。这种攻击有别于军事和情报攻击，恐怖攻击的目标在于中断正常的生活和制造恐怖气氛，而军事和情报攻击被用来获取秘密信息。计

算机恐怖攻击的目的可能是控制电厂、控制电信或者造成电力中断。

⑤恶意攻击 Grudge Attacks（报复）

恶意攻击可以对组织机构或个人造成破坏。破坏可能是信息的丢失或信息处理能力的丧失，也可能是组织机构或个人名誉的损害。恶意攻击的动机通常来自于不满，并且攻击者可能是现在的或以前的员工，也可能是希望组织机构不能正常运作的人。

⑥兴奋攻击 Thrill Attacks（破坏）

兴奋攻击是由具有很少技能的破坏者所发起的攻击。缺乏自己设计攻击的能力的攻击者常常会下载使用某些程序来进行攻击。这些攻击者常常被称作“脚本小子”script kiddies，因为他们只运行他人的程序或脚本而发起攻击。这些攻击的动机是闯入系统的极度兴奋。如果你是兴奋攻击的受害者，那么所遭受的最常见打击就是服务的中断。虽然这种类型的攻击者可能会破坏数据，但是其主要的动机还是破坏系统，并且可能使用该系统对其他受害者发起拒绝服务攻击。

A.4 数字取证 （例如： 介质、网络、软件和嵌入式设备）

1.基础知识

国际计算机证据组织(International Organization on Computer Evidence, IOCE)，目的是制定收集和处理数字证据的国际原则，从而使各国的法庭都同样认可和使用这些证据。

数字证据科学工作组(Scientific Working Group on Digital Evidence, SWDGE)，美国的机构，也可以确保取证团体之间的一致性。

警务管理协会(Association of Chief Police Officers，ACPO)，提供了标准的电子取证流程和方法指南。

IOCE/SWDGE 的取证 6 大原则是：

①合规性。处理数字证据时，必须遵循所有通用取证的程序原则。

②完整性。查封数字证据时，所采取的行动不得改变证据。

③有能力。访问原始数字时，该人必须受过专门培训。

④可审计。保管数字证据时，扣、访、存或传等所有活动，必须被记录，以供审查。

⑤可问责。某人拥有证据时，要对其一切操作行为负责。

⑥通用性。任何的组织机构，扣、访、存或传证据必须合规，并承担责任。

2.介质分析 Media Analysis

介质分析是计算机取证分析的一个分支，就是识别和提取各种存储介质中的信息。应当为原始介质创建 2 个副本：一个主镜像，这是保存在库中的控制镜像；一个工作镜像，它用于分析和证据收集。

3.网络分析 Network Analysis

网络取证(分析)这个术语是在 1997 年由 Marcus Ranum 提出，指的是分析和审查网络日志和网络活动数据来找出潜在的证据。数字证据的大范畴包括了许多类别，如软件取证/分析，网络分析或网络取证。网络活动分析是一种功能，在任何事件响应的情况和过程模型都是相同的，在之前的“事件响应’一模块中已经讨论过。关键特征是证据的有效管理和处理(即监管链)，是关注任何来源的证据在法律程序中是否被接纳。

4.软件分析 Software Analysis

软件分析和取证是指分析和检查程序代码。被分析的代码可以以源代码的形式一编译后的代码(二进制文件)，或机器代码。反编译和逆向工程技术经常被用作这个过程的一部分。软件分析等调查活动包含恶意软件分析、知识产权纠纷、版权侵权行为等等。分析的目标包括作者标识，内容分析/语境(有效载荷)，和上下文分析。

5.硬件和嵌入式设备的分析 Hardware/Embedded Device Analysis

硬件和嵌入式设备的分析通常涉及到移动设备，如智能电话或个人数字助理(PDA)，在笔记本或台式计算机的主板可以发现标准的硬件和固件如 CMOS 芯片用于控制基本功能，同时需要被取证拍摄并进行检查。嵌入式设备的成像是需要专用的工具和技术。需要注意的是，许多嵌入式设备无法读取或复制，他们希望获得和不改变这些重要信息。

6.作者的身份识别

作者身份识别，或者更准确地说作者归属，试图确定谁是创建或撰写软件/程序的作者(这是一个个人或小组工作)。代码检查的线索有，编程风格，程序语言，开发工具包使用嵌入的注释和地址等。基本的理论是，编写代码类似于散文写作，每个作者都有独特的风格和怪癖，可以让研究者区分各种潜在的犯罪嫌疑人。

7.内容分析

内容分析以分析系统代码为目的。以一个木马程序为例，要重点确定用来做什么样的攻击，文件应安装在受感染系统的哪个位置，开放什么样的端口(出口和入口)，如何识别上游目标地址，什么信息被批量上传发送或本地存储等等。内容分析也用于知识产权纠纷案件。在这些情况下，检查源代码或反编译二进制需要一个辛苦的检查，用来确定两个程序之间的相似性。研究者往往要求提供相似的程序，专家基于什么基础提供意见。内容分析处理相对于案例环境中发现一元视图可疑软件的影响。理解内容可以协助分析，可用于组织发现风险或对受害者进行真实评价。

B.理解调查类型的要求

详细内容见第一域 D 章节

调查的类型有 5 种，就是后面这 5 种，没什么考的内容。

B.1 运营

操作型调查 Operational Investigations

企业组织的内部业务问题，一般是系统运维、内部审计等人员干的，只针对内部的信息系统，不涉及其它企业也不涉及政府，其目标是解决系统问题、业务问题和管理问题。所以取证工作并不严格，通报事件并解决就行了，除了个别事件是涉及外部、严重的犯罪的，那就不是简单的事了。

B.2 刑事

犯罪调查/刑事调查 Criminal Investigations

犯罪调查通常是由法律执行者进行的，针对违法行为的调查。犯罪调查的结果是指控犯罪和这些指控在刑事法庭的控诉。刑事调查必须遵循非常严格的证据收集和保存的过程。

B.3 民事

民事调查 Civil Investigations

民事调查通常不涉及执法，是企业内部和企业之间请律师来自己解决问题。民事调查的证据收集标准并不像那些在犯罪调查中要求的那么严格。

B.4 法规

监管调查 Regulatory Investigations

政府职能机构来做的调查，就是政府认为个人或企业可能违反法律时，提起公诉并执行监管调查。

B.5 电子发现

电子发现/电子披露是一种独特的网络调查。

1.电子发现 Electronic Discovery

任何组织有责任保留各种有用的电子证据，即日志记录什么的，并在法律需时通过“电子发现”过程来提供和分享信息。这个发现的过程包括纸质档案和电子记录的查找，以及各种自动化、数字化、网络化的数字取证或电子发现(e-Discovery)过程。

2.电子发现参考模型（EDRM）Electronic Discovery Reference model

EDRM 的流程步骤：

信息管理=>身份识别/鉴定=>①保护+②收集=>①处理+②审查+③分析=>制作=>呈现/演示

在捕捉嫌疑人的活动中，诱骗是合法的和道德的，而圈套既不合法也不道德。蜜罐用来避开攻击是合法的，用来提起诉讼是非法的。也就是说伪装保护自己的可以的，钓鱼执法搞人是不行的。

C.实施日志和监测活动（行为记录和监控活动）

考日志重点涉及到 IDS/IPS、SIEM、连续监测服务 CMaaS、出口监控、数据泄漏/丢失保护（DLP）。都在后面章节里讲了。当然也有防火墙、补丁管理、防病毒什么的，都类似。

1.日志技术

日志记录是将事件的信息记录到日志文件或数据库的过程。日志通常被称为审计日志，而日志记录通常被称为审计日志记录。不过日志记录只是记录事件，而审计会检查其所处环境。

2.保护日志数据

如果攻击者可以修改日志，他们便能够擦除自己的活动痕迹。要保护好。

3.监控技术 Monitoring Techniques

监控是一种检查信息日志并寻找具体某些细节的过程。工作人员可以手动查看日志，或使用工具来自动处理过程。监控是必要的，以检测恶意行动，以及入侵和系统故障。它可以帮助重建事件，提供起诉的证据，并创建分析报告。日志分析是监测过程中一种详细且系统化的模式，日志分析能够分析监测记录信息的趋势、模式，还能够分析未经授权的、非法的、违反政策的活动。日志分析不一定是对一个事件的响应，而是一个周期性的任务，它可以检测潜在的

问题。

4.审计 Auditing

许多时候，一个组织将会通过审计的方式评估其安全政策和相关的访问控制。审计是对**环境**有条理地检查或审查，以确保其符合法规和并能够检测异常、未经授权的事件，或犯罪。它验证部署在环境中的安全机制能否提供足够的安全性。测试过程确保工作人员遵循由安全策略或其他规则所制定的要求，并且在部署的安全解决方案中不存在重大漏洞或弱点。

审计在信息技术安全性背景下有两种不同的的含义，即审计与审查，认识差异是很重要的。

①审计是指利用审计日志和监控工具来跟踪活动。例如，当任何用户访问文件时，审计日志可以做出记录，并记录该用户的使用过程。（找用户行为的问题）

②审计也指检查或评估。具体地说，审计是对一个特定的过程或结果的检查或评价，以确定一个组织是否遵循特定的规则或准则。（找管理机制的问题）

审计也有几种类型：

①检验审计 Inspection Audits

安全信息技术环境很大程度上依赖于审计，将其作为一个侦探安全控制机制，以发现和纠正漏洞。用于访问控制的两个重要的审计分别是访问审查审计和用户权限审计。

②访问回顾审计/访问审查审计 Access Review Audits

许多单位定期进行访问审查和审计，以确保对象访问和帐户管理符合安全策略要求。这些审计能够检查用户。以确保其没有过多的权限，并能够适当地管理帐户。他们确保监管流程和程序都正常运行，人员会对他们进行跟踪。就是要对访问控制的管理和审查进行审计

③用户权限审计 User Entitlement Audits

用户权限是指授予用户的权限。用户需要权利和权限来完成工作，但他们只需要有限数量的特权。要遵守最小特权原则。

④特权组审计 Audits of Privileged Groups

要确保高级别小组成员只有在必要时才使用他们的高特权帐户。审计可以帮助确定这些人员是否遵循这些政策。

5.安全审计和复核 Security Audits and Reviews（搞清区别）

安全审计有助于帮助单位确定正确地实现了安全控制。访问审查审计能够评估访问控制的有效性。这些审计确保帐户管理适当，没有过多的权限，并在需要时会被禁用或删除。下面是一些常见的检查项目（在该域后面的 I、J 等章节时会逐个讲这些内容的）：

①补丁管理 Patch Management。（补丁可用）

补丁管理审查能够在补丁发布后，尽可能快的对其进行评估、测试、批准、部署和验证补丁程序。在补丁管理审查或审计中漏洞扫描报告是很有价值的。（补丁管理的过程不包括“部署所有补丁”这个内容。）

②漏洞管理 Vulnerability Management。（漏洞已补）

漏洞管理审查能够确保漏洞扫描和评估定期按照既定的准则定期执行。审查将验证在扫描中发现的漏洞问题已经得到解决。

③配置管理 Configuration Management。（应对变更）

系统可以定期进行审核，以确保原始配置不被修改。配置管理审计可以检查任何变更的日

志，并验证此变更是否经过授权。

④变更管理 Change Management。（实施变更）

变更管理审计能够确保变更符合单位变更管理政策。其中通常包括中断审查，以确定原因。由未经授权的变更导致的中断意味着变更管理程序需要改进。

6.审计跟踪/行为记录 Audit Trails（事件溯源）

审计跟踪指的是关于事件和突发事件的信息，它存储在一个或多个数据库或日志文件中。审计跟踪提供了系统活动的记录，并可以重建导致安全事件的活动。安全专家提取事件的审计线索来证明或反驳责任信息。审计跟踪允许安全专业人员检查和跟踪事件的正向或反向顺序。使用审计跟踪是一种被动的检测性安全控制形式，只是作为一种威慑力量。

C.1 入侵检测与预防

详见 H.2 章节

C.2 安全信息与事件管理 Security Information and Event Management

1.安全信息和事件管理

许多单位使用一个集中的应用程序来自动监控网络上的系统，如安全信息和事件管理系统/安全事件信息管理系统（SIEM）、安全事件管理系统（SEM）和安全信息管理系统（SIM）等。这些工具为单位提供了对系统事件的实时分析。例如，SIEM 可以监视一组电子邮件服务器，会检查某事件以确定它是否是一个和利益有关的项目，并根据事件的严重性，依次提高向管理员的告警。该工具还可以从目标系统收集所有的日志，并使用数据挖掘技术来检索相关的数据。SIEM 产品的目的是提供一个公共平台，进行日志收集，整理，实时分析，允许更有效的响应。他们还可以提供来自多个源的日志信息报告。安全信息和事件管理(SIEM)是一个术语，用来描述一组技术析综合信息系统的访问控制和选择存储活动的相关性，用于分设备日志和系统信息的收集。日志和系统信息可以以各原因来收集。SIEM 和日志分析工具是快速将两个区域合并成一个功能空间，通常一个 SIEM 具有以下特点：

①存储来自不同系统的原始信息日志

②汇总单个存储库的信息

③规范化信息的比较更有意义

④分析工具可以处理映射和提取目标信息

⑤警报和报告工具

2.日志管理系统

日志管理系统比较相似：他们有收集日志和提供报告的能力，虽然他们的重点往往是对日志信息的历史分析，而不是实时分析。他们可以结合 SIEM 解决方案提供历史和实时功能。

3.SIEM 和日志管理

在这两种情况下，必须谨慎地对管理日志信息进行安全操作，必须保持严谨的日志存储和归档。对于大多数 SIEM 或日志管理系统而言，对信息量做出一个实际的限制，他们就可以分析一次或产生针对的报告。对于大多数系统，有一种解决方案，只有一小部分的剩余日志可以转移到在线存储，这样可以进入长期存储或归档。这些解决方案存储在线日志可以长达 10 到 180 天，他们移到一个在线或近乎线性的存档长达一年，然后移动日志进行长期备份，去覆盖

保留期的剩余部分。在这段时期结束时，安全操作员负责使用定义的数据处理程序和工具来确保旧的日志信息、被正确处理。

C.3 连续监测 CMaaS

持续监测也是云服务的一种，是一种风险管理的方法，允许一个机构对其风险状况作出持续地描述。**持续监测作为一种服务(CMaaS)**是关于一个感兴趣领域的持续监测。最初需要此服务的是美国联邦政府重点的网络防御和正在建造的基础设施服务需求。连续诊断和缓解（CDM)项目提供专业化的信息技术(IT)的工具，并使用 CMaaS 打击针对平民“.gov”网络的威胁。CDM 方法遵循合规报告和应对实时威胁国家的基础网络，自动化监控工具将允许获得整个联邦企业的安全相关信息并进行分析。

C.4 出流监测（例如：数据丢失防护、信息伪装、数字水印）

出流监测/出口监测是指监测传出的流量，防止数据泄露，也就是防止单位数据未经授权的外泄。防止数据泄露的一些常见的方法有使用数据丢失防护技术，寻找隐藏的企图，并利用水印检测未经授权的数据。

1.数据泄露保护 Data Loss Prevention

数据丢失防护(DLP)系统能够检测和阻止数据地露的企图。这些系统有扫描数据、寻找关键字和数据模式的能力。DLP 系统有两种主要类型：基于网络的 DLP 和基于终端的 DLP。DLP 系统通常具备进行深层次检查的能力。例如，如果用户将文件压缩成 ZIP 压缩文件，仍然可以检测到关键词和模式。（国安局什么的部门都有这种系统）

DLP 有三个关键目标：

①企业敏感信息的查找和分类存储（存储数据）（静态数据）Data at Rest。

②监控和控制企业网络敏感信息的流动（网络数据）（动态数据）Data in Motion。

③监视和控制用户系统敏感信息的流动（用户数据）（数据使用）Data in Use。

DLP 有 5 个基本功能：

①策略建立和管理 Policy Creation and Management;

②集成目录服务 Directory Services Integration;

③工作流管理 Workflow Management;

④备份和恢复 Backup and Restore;

⑤报告 Reporting。

这些目标与三种类型的信息相关：静态数据、动态数据和数据的使用。相应解决方案如下：

①静态数据 Data at Rest：大多数的 DLP 系统利用爬虫，搜索已进入 DLP 管理控制台的数据，基于一组有规则并记录其位置的特定信息集合。也就是信息过滤系统。

②动态数据(网络) Data in Motion (Network)：使用特定的网络设备或嵌入式技术选择性地捕获和分析网络流量，检查通过网络发送的信息，这种能力的核心是一个称为深层数据包检测(DPI)的方法，使 DLP 数据可以动态组件来完成这些任务。DPI 通过超出一个分组的基本报头信息来读取数据包的有效载荷内的内容。这种 DPI 功能允许 DLP 系统来检查传输中的数据，并确定内容，源和目的地。如果检测到敏感数据流向一个未经授权的目的地，DLP 解决方案具

有提醒和阻塞数据流，再根据中央管理组件中定义的规则集进行控制。也就是流量分析系统。

③使用数据(终端) Data in Use (End Point)：DLP 最具挑战性的方面可能是数据的使用。数据的使用主要是指监控终端用户的数据运动并采取行动是否需要将数据复制到 U 盘，将信息发送到打印机，甚至在应用程序之间剪切和粘贴。DLP 解决方案通常通过使用称为代理的软件程序来实现这个功能，也就是主机监控系统。

2. 消息隐藏/信息隐藏 Steganography

隐写术 Steganography 指的是在一个文件中嵌入消息。一般写入图片、声音、视频什么的，也可以使用隐蔽通道。隐写术涉及 3 类组件：

①载体——内部具有隐藏信息(有效载荷)的信号、数据流或文件。

②隐写介质——将信息隐藏在内的介质。

③有效载荷——要隐藏和传输的信息。

下面的公式描述了一个通用的隐写过程：

覆盖介质+隐藏数据+密钥=隐秘介质

3. 水印 Watermarking

水印指的是在纸上嵌入不容易感知的图像或图案，它经常被用来防止伪造货币，也用来防止了单位文件的泄露。数字水印是一种比较先进的水印方式。数字水印是一种在数字文件中秘密嵌入的标记。例如，一些电影公司对发送给不同分销商的电影嵌入数字水印，每个副本都有一个不同的标记且可以追踪哪个分销商收到了哪份副本。如果有分销商发行盗版电影，工作室便能够确定是哪家分销商。

D. 保护资源的供给安全（通过配置管理确保资源的供应和安全）

D.1 资产清单 （例如：硬件、软件）

有形资产和无形资产很容易理解，CISSP 一般会提到两个单词：

①硬件 hardware：就是设备啦。

②介质 media：硬盘、软盘、光盘、纸张、胶片等。

清单有助于验证系统、软件和网络上设备的完整性，从两个视角了解网络组件的硬件版本。此外在执行网络扫描时，对比清单，可以发现网络中未经授权的设备。

1. 硬件清单 Hardware Inventories

贯穿设备的整个生命周期，许多组织使用数据库和库存应用程序来清点库存和跟踪硬件资产。例如，条形码系统可以打印条形码并放置在设备上，也能使用无线射频识别（RFID)标签。在设备处理之前要进行人工净化：清除设备中所有数据，以确保未经授权的人员不会访问到敏感信息。

2. 软件清单 Software Inventories

软件清单至少包括：软件名称/软件供应商(和经销商如合适)、密钥或激活码(注意，如果有硬件密钥)、许可证的类型和版本/祥拥有许可证/许可证失效、移动的许可、组织软件库或资产管理/安装软件的联系人等。

也应该对每个设备配置维护清单，设备如防火墙，路由器和交换机，可能会有成百上千的配置。要正确记录和跟踪更改这些配置清单，以保证对网络提供完整性和可用性。

3.软件许可 Software Licensing

购买软件，要使用许可证密钥来激活软件。因此，对组织来说任何类型的许可证密钥都是非常重要的，需要加以保护。

D.2 配置管理

配置管理 Configuration Management，CM 有助于确保系统处于一致安全的状态，并在其整个生命周期维护这种状态。它是评估、协调、批准或不批准，以及实施**变更**，用以构建和维护软件系统的过程。

1.基线 Baselining

基线是一个起点。在配置管理中，它是一个系统的初始化配置。管理员为了满足不同需求经常在完成系统部署之后修改基线。然而，当系统被部署在一个有安全基线的状态下，系统会更安全。基线就是组织自己的针对系统安全的一套安全配置规范。例如，微软操作系统包括**组策略**。管理员可以单次配置一个组策略，之后组策略会自动将设置应用到域中的所有计算机上。

基线有 2 个：配置基线和安装基线（镜像）。

2.用镜像创建基线 Using Images for Baselining

许多组织使用镜像来创建基线，有三个步骤：

①初始。起初，管理员在计算机上安装操作系统和所有所需的应用程序，并对系统进行相关的安全配置以满足单位的需求。在继续下一步之前，将进行人工测验来确保系统正常运行。

②镜像。接着，管理员制作系统的镜像，存储在镜像服务器中，或外部存储设备。

③部署。然后，根据需要，使用镜像来部署各个用户系统，使所有系统的整体配置同基线系统是相同的。

所以，每个单位都应该裁减定制适合自己的、安全的操作系统，并做成镜像安装文件，确保所有的终端都安装了自主可控的，符合安全基线的系统和软件。

3.配置管理的软件能力成熟度模型

SEI 能力成熟度模型集成 CMMI，系统工程和软件工程的 1.1 版(CMMI-SE/SW,V1.1)列出了一个组织有助于 CM 能力的最佳实践[SEI2000A]：内容就不粘贴了。

4.补丁和漏洞管理 Patch and Vulnerability Management

都很好理解，不多说。

D.3 物理资产

物理资产在信息技术硬件之外，包括所有的物理设施，如一个组织的建筑和它的内部设施。保护实物资产的方法包括栅栏、路障、门锁、安保、闭路电视(CCTV)系统等。

D.4 虚拟资产（例如：软件定义网络、虚拟 SAN、来宾操作系统）

为了大幅节约成本，组织逐步使用越来越多的虚拟化技术。软件定义一切 Software defined everything (SDx)是指以软件代替硬件的虚拟化趋势。在此概念下的虚拟资产包括：

①虚拟机(VMs)Virtual Machines：虚拟机类似于物理服务器上的客户操作系统。

②软件定义网络(SDNs) Software-Defined Networks：能够将控制平面从数据平面(或转

发平面)中分离出来。控制平面使用协议来决定向哪里发送信息，而载有规则的数据平面决定是否转发信息。不同于传统的网络设备如路由器和交换机，SDN 控制器使用能够接收控制器指令的简单的网络设备。这消除了一些与传统的网络协议相关的复杂性。

③虚拟存储区域网络(VSANs) Virtual Storage Area Networks：是含有多个存储设备的专用高速网络。他们经常与需要高速访问数据的服务器一起使用。很久以来，由于其复杂的硬件要求，SAN 的价格居高不下。VSANs 通过虚拟化，降低了成本。

虚拟化中的主要软件组件是管理程序。虚拟机管理程序管理虚拟机、虚拟数据存储和虚拟网络组件。作为物理服务器上的一个附加的软件层，它也是另外的一个攻击面。如果攻击者能够破解物理机，那他就可以访问托管在物理服务器上的所有虚拟系统。

D.5 云资产 （例如：服务、虚拟机、存储、网络）

基于云的资产包括一个组织使用云计算访问的任何资源。云计算是指几乎可从任何地方提供按需访问的计算资源，且云计算资源高度可用、易于扩展。搞清楚什么是 SaaS、PaaS、IaaS，一般都有云服务提供商(CSP) cloud service provider 来负责。第三域 E.5 章节已经讲过那些云了。再讲几种云部署的模型：

①公共云模型包括——可用于任何消费者租用的资产，并由外部 CSP 管理。

②私有云部署模型包括——单位可以使用自己的资源创建和管理私有云。该单位负责所有维护。然而，一个组织也可以从第三方租赁资源并按照服务模型(SaaS，PaaS 或 laaS)分割维护职责。

③社区云部署模型——为两个或多个单位提供云基础资产。维护责任根据对资产和服务模型的管理来分配。

④混合模型包括——两个或两个以上的云组合。类似于社区云模型，基于对资产和服务模型的管理，维护责任共享。

D.6 应用 （例如：工作负荷或私有云、Web 服务、软件即服务）

E. 理解与应用安全运营的基础概念

准确的讲，这章是关于安全运作、安全操作的内容，不是安全运营，因为运营层次更高，有部分管理的职能。

1.概念区分

①运行安全（Operations Security），是指网络和系统保持安全、稳定、可靠、高效的运行状态，能有效支撑保障各项公司业务的正常开展。（系统运行很安全）

②安全运营（Security Operations），是为了确保网络和系统的运行安全可靠，而实施的一系列专业安防运维工作。也就是各单位的安防部门要干的事，如经常要做的预防（Prevent）问题、监测（Detect）问题和处理（Correct）问题等。（安全运维很到位）

③操作/运营（Operation），这是个动词，就是对在用的网络或系统进行运行维护的具体工作，这里主要指安全方面的维护。虽然有许多安全机制来保护系统，但也会出现很多故障，所以必须进行维护操作。很多单位的安防中心就干这个事。

④可信路径，为特权用户提供可以信赖接口的功能，目的是提供一种方法来确保任何通信

路径不被截取或损坏。例如，当用户登录到本地系统，他的凭据可以安全地通过从用户界面到访问控制子系统来共享，这是很重要的。然而，许多攻击可以截获，泄露，或操纵，专门攻击这样的信任路径重定向到另一个通道。这种攻击如果成功，那么会提高了攻击者的权限水平，所以使用特权用户帐户非常危险。（这就是说登陆界面是可信的，不能被篡改）（可信路径在讲操作系统内核与外界的通信时也有）

这章也涉及到故障安全机制的 Fail-Safe 和 Fail-Secure 概念，讲了好几遍了，很好理解，在 K.2 章节有。

2.主要内容

总的来说，第七域的安全运营可以理解为是一系列的针对公司信息安全防护业务的管理与运维工作。一般重点关注四个方面的工作（美国知识其实并不适用于中国）：

①确保运维灵活、高效（弹性）maintaining operational resilience：就是及时有效的预防、监测和应对突发事件，降低负面影响。

②保护有价值的资产 protecting valuable assets：包括人、物、钱、数据。

③实施访问控制（账号管控）controlling system accounts：避免权限滥用或误用。

④有效管理安全服务 Managing Security Services Effectively：提供安防服务，实施变更管理，分析评估报告什么的。

E.1 需者方知/最小权限原则（例如：权利、聚集、信任传递）

第五域的 E 章节已经把需知、最小特权、职责分离都说过了，这里不想再说了，本来就很容易理解。还有聚合、信任传递的概念，也都说过了。

考题中关于信任传递会问到几种模式：

①单向信任 one-way trust：你的就是我的，但我的还是我的，不给你。

②双向信任 two-way trust：互信互访。

③信息可传递 transitive trust：信任可延动态目录树传递。

④信任不可传递 nontransitive trust：信任固定，不能延动态目录树传递。

E.2 职责分离

1.职责和责任分离 Separation of Duties and Responsibilities

职责和责任分离确保没有单个人能控制一个关键功能或系统全部，但如果有共谋或串通违反组织的行为，分离也没用，不过能极大的增加串通的难度和风险。

①特权分离 Separation of Privilege

高等级的特权必须要分离。

②职责划分 Segregation of Duties

有利益冲突的职能必须要分离。

③双人控制 Two-Person Control

制类似于职责划分，是指关键任务必须由两个人同时完成。

在讲密钥管理时，也会讲到职责分离、双重控制、知识分离：

④双重控制 dual control。2 个或多人要同时一起来完成一个流程。（同控）

②知识分离 split knowledge。密钥或资产要分发给不同的人来保管。（分管）

E.3 监控特殊权限（例如：操作员、管理员）

确保账户及其权限进行适当分配和定期审查。**常用的监控手段**有：

①背景调查：定期的背景调查确保他或她的职责分配和授予个人的级别是适当的。

②帐户验证：一个人从组织中离开，应该从系统中删除这些不活动的帐户；长期休假或临时调离，应禁用这些不活动的帐户。

③岗位轮换：岗位轮换可以减少个人之间共谋活动的风险。

要重点监控的特殊角色有：

①系统管理员 System Administrators

最小特权：系统管理员并不需要访问组织中的每个系统和功能。

监控：系统管理员的行动应记录并发送至不受系统管理员控制的一个独立系统。日志应该按配置管理要求进行更改并进行审查，以确定只有经过授权的行为才能被发生。

防止欺诈行为：管理员不应该从事恶意活动并且没有欺诈的能力。

它是最高权限，所以没有职责分离。

②操作员 Operators

操作员拥有很高的权限，但低于系统管理员，如果使用不当，这些特权可以用来规避系统的安全策略，因此，应该监控这些特权的使用并进行日志审计。

最小特权：并不需要访问组织中的每个系统和功能。

监控：行动应记录并发送至不受操作员控制的一个独立系统。日志应该按配置管理要求进行职责分离，更改并审查，以确定只有经过授权的行为才能被发生。

职责分离；不应该从事恶意活动并且没有串通作案的能力。

背景调查：应该进行背景调查，以确定这个操作者是否曾经有过勒索和敲诈行为。

③安全管理员 Security Administrators

安全管理员是对系统安全操作进行监督的角色。安全管理员和系统管理员有必要一起进行安全设置工作，因为一个不适当的配置可以影响系统或网络的正常运行。这些管理员通常比系统管理员的权限要少。这是必要的，以确保执行职责分离。安全管理员提供一种权力制衡，为系统管理员提供审计和审查其活动。

④帮助/服务台人员 Help/Service Desk Personnel

帮助/服务台人员负责为所有用户提供一线的支持。作为技术支持人员往往需要有重置密码的能力，有必要对他们进行监控和背景调查。

第一域的 B.3 章节、第二域的 B 章节等，到处都讲到了“数据所有者”等等各种角色，前后关联起来看，数据所有者、系统监管员、安全管理员等的关系是必考的。

E.4 岗位轮换

1. 工作轮换 Job Rotation

工作轮换简单的讲就是轮换职责，或者至少某些工作职责被轮换到不同的雇员。这可以实现并行审查、减少欺骗并促进交叉培训。工作轮换既能作为一个威慑也能作为一个检测机制。

提供人员的备份（Backup）和冗余（Redundancy）。

2.强制休假 Mandatory Vacations

这将提供一个并行互审的形式，并且有助于检测欺诈和共谋。该策略确保了其他雇员接替一个人的工作职责至少一个星期的时间，如果一个雇员涉及欺诈，接替该职责的人将会发现该欺诈。强制休假既能作为一个威慑也能作为一个检测机制。强制假期具有突然性(Unexpected)，使欺诈者（Fraud）没有时间来掩盖欺诈痕迹。

E.5 信息生命周期

信息生命周期是用于管理和存储数据的方法，信息随时间而改变，必须进行相应的管理。

1.生命周期一般分六个阶段：

创建和接收——分发(存储/备份)——使用——维护——披露——处置(转让，安全处理)

安全控制要保护整个生命周期内的信息，包括标记、处理、存储和数据恰当销毁。

①标记 Marking Data

数据标志(或标签)确保用户能很容易的识别数据的价值。除了外部系统的标记外，企业组织也经常配置壁纸和屏幕保护来清晰的表明在系统中处理数据的等级。

②处理 Handling Data

数据处理主要涉及到数据的传输，并且关键是在传输过程中提供与数据存储时相同级别的保护。在发送数据之前对其进行加密来提供这种数据保护。

③存储 Storing Data

数据存储的位置需要得到保护以防止丢失。数据主要存储在磁盘驱动中，并且需要人去周期性的备份有价值的数据。存储敏感信息的备份位于一个位置，而其拷贝存放在另一个存储位置。物理安全机制防止这些备份被偷盗。有关环境的控制防止数据由于腐蚀而丢失。

④销毁 Destroying Data

数据当数据不再需要时销毁数据，且以一种数据不可读的方式来销毁。

2.信息所有者 Owner（考点）

创建信息的人必须对该信息直接负责，这个个体或群体被认为是“信息的所有者”。信息所有者通常具有以下职责：

①确定信息对组织使命具有影响；

②了解信息的重置成本(如果它可以被取代)；

③决定哪个组织需要这些信息和在什么情况下应该发布这些信息；

④了解该信息是不准确的或是不再需要的，应当销毁。

3.分级 Classification

按照敏感度即信息密级来区分。显然信息所有者必须与信息安全人员合作，对信息进行分级，使用术语“机密”，“秘密”，“限制”或“敏感”等 来标记信息。分级关注的是**访问**。

4.分类 Categorization

按照影响度即信息的重要性来区分。分类是确定在组织中信息的保密性，完整性或可用性损失影响的过程。分类的标准是根据：价值、寿命、使用期和人员关联。分类关注的是**影响**。

5.保留 Retention

最后，所有的信息最终必须结束。组织经常囤积旧信息，有些法律也要求必须保留数据一定的时间。

6 残留 Remanance

以某种形式删除数据之后，磁盘还会有剩磁，可以进行物理恢复的数据。

具体在第二域 C.3 章节里讲了。

E.6 服务水平协议

服务水平协议，也称为服务级别协议 SLA(service level agreement)，是一个组织和外部实体(如供应商)之间的一份协定，在与第三方合作时，应该清晰的知道自己的需求，并确保 SLA 中包含这些需求。SLA 是企业和外部供应商之间，但也可能是在公司内的个部门之间(这些被称为操作水平协议，或者 OLA)。除了一个 SLA 之外，公司常常使用一个备忘录协议 memorandum of understanding(MOU)或者一个互联安全协议 interconnection security agreement (ISA)，它们是非正式的，不包括违约的处罚，起到的约束作用有限。

SLA 应该包括两个方面的组件：服务和管理。

服务内容包括提供服务的细节，标准时间窗口的服务水平，每一方的责任，升级程序，权衡成本/服务等。（提供什么服务）

管理要素应包括定义测量的标准和方法，报告流程，内容和频率，争端解决的过程，赔偿条款等，以及更新协议的机构与方法等。（服务质量怎么样）

SLA 不包含保密的、机密性！这是属于保密协议 NDA(non-disclosure agreement)的。

F. 利用资源保护技术

F.1 介质管理

介质管理（media）是指采取措施保护介质和存储在介质上的数据的步骤。介质是指可以保存数据的任何事物。它包括磁带、CD 和 DVD 光盘、便携式 USB 或 FireWire(火线)驱动器、外部 SATA(eSATA)驱动器、内部硬盘、固态硬盘、USB 闪存驱动器等等。

国外也这么分：软拷贝介质（电子的、数字的）和硬拷贝介质（物理里纸张、胶片等）。

1. 闪存驱动器控制 Controlling USB Flash Drives

采购 USB 闪存驱动器要限制在特定品牌范围内

2. 磁带介质设备 Tape Media

磁带常因腐蚀而很容易损坏。最佳的方法就是保存至少两份备份，一份保存在外部，必要时立即使用；第二份保存在安全的位置。磁带还不能暴露于磁场、高温中。

3. 移动设备 Mobile Devices

移动设备包括手机和平板电脑等。这方面的安全讲的很多了，每个单位都有措施。

4. 介质管理保护方法包括：

加密——在传输过程中加密——移动介质——云存储——虚拟存储

5. 虚拟化存储的不同类型

虚拟存储是多个网络存储设备的物理存储池，由一个从中央控制台管理。虚拟化的好处是，更便宜的硬件可用于提供企业级存储的功能。虚拟存储化可以更容易地帮助存储管理员执行备

份，存档、和恢复任务，并可以在较短的时间，以掩饰一个存储区域网络(SAN)的实际复杂性。

虚拟化存储的不同的类型包括：

①基于主机的储存

基于主机的虚拟化需要在主机上运行额外的软件，作为一个享有特权的任务或进程。在某些情况下，容量管理是建立在操作系统上，而在其他情况下，它是作为一个单独的产品。卷(LUN)提交给主机系统，由传统的物理设备驱动程序来处理。然而，一个软件层(卷管理器)驻留在磁盘设驱动程序之上截取 I/O 请求，并且提供了元数据的查询和 I/O 映射。大多数现代操作系统都内置有某种形式的逻辑卷管理(在 Linux 中它被称为逻辑卷管理器或 LVM；在 Solaris 和 FreeBSD、ZFS 使用 zpool 层；在 Windows 逻辑磁盘管理器或 LDM，执行虚拟化的任务。

②基于设备的存储

主存储控制器提供虚拟化服务，并允许其他存储控制器直接连接。可能来自相同或不同的供应商来实现这些功能。主控制器将提供集中和元数据管理服务。它也可以跨控制器提供虚拟化复制和迁移服务。

③基于网络存储

在基于网络设备的存储虚拟化操作(通常是一个标准的服务器或智能开关)，使用 iSCSI 或光纤通道(FC)网络连接为一个 SAN。这些类型是最常用实现虚拟化的设备。虚拟化设备位于 SAN 中，并提供主机之间的抽象层，执行 I/O 和提供存储控制器存储容量。

④存档和离线存储

就是备份和恢复、归档。

6.记录管理 RIM

记录信息管理（RIM）：ARMA 国际定义保护的企业信息的基本活动，保护硬拷贝记录和软拷贝记录。这是一个用来管理信息的方法和工具。就是要保护好重要的数据资产，有 2 种类型：

①硬拷贝记录。就是纸张、胶片什么的，保护方法就是扫描。

②数字记录。通过信息系统来读取和呈现。

F.2 硬件与软件资产管理

软件托管协议 Software Escrow Arrangements 是一种特殊的工具，可以对公司起到保护作用：它避免公司受软件开发商的代码故障的影响，以便为产品提供足够的支持，还可以防止出现由于开发商破产而造成产品失去技术支持的情况。在软件托管协议下，开发商将应用程序源代码的副本提供给独立的第三方组织机构。然后，第三方用安全的方式维护源代码副本备份的更新。这个经常考到，就是要给第三方的软件开发找一个监理人。（考点）

第八域 B.3 章节也讲了。

G.开展事件管理（实施事件响应）

事件响应的主要目标是尽量减少事件对组织的影响。

1.事件界定 Defining an Incident

事件有 2 个英文单词：Event 和 Incident

①Event：特定时间内发生的任何事件都称为事件。不过也有安全教材把 event 也看成是

incident 安全事件了，即被发现、验证和记录的负面事件。管它的，好坏都对。

②Incident：这是指事故，即对数据的机密性、完整性和可用性具有负面影响的事件。

反正，在 CISSP，事件全都是指计算机安全事件，即 Incident。

2.事件响应步骤 Incident Response Steps

SP 800-61 是学习更多关于事件处理的极好资源，但它确定事件响应生命周期分为以下**四个步骤**：①准备，②检测和分析，③遏制、消除和恢复，④事后恢复。

CISSP CIB（Candidate Information Bulletin）中概括的管理事件响应涉及**五个步骤**：其实就是本章后面 7 个内容的中间 5 个步骤。（G.1 到 G.7）

①Detection②Response③Mitigation④Reporting⑤Recovery⑥Remediation⑦Lessons Learned

①检测；---②响应；--③缓解；----④报告；---⑤恢复；--⑥补救；-----⑦教训

也有教材这么分的步骤：

①诊断/分类(Triage)、②调查(Investigation)、③遏制(Containment)、④分析(Analysis)和追踪(Tracking)、⑤恢复(Recovery)

3.事故/事件的类型 Common Types of Incidents

①非法扫描 Scanning

扫描攻击通常是先于其他更严重的攻击进行的侦察攻击。

②非法访问 Compromise

非法访问指的是对系统或系统存储的信息进行的未授权访问。而且，合法用户 ID 的被恶意使用是难以检测。

③恶意代码 Malicious Code

病毒、间谍软件等等。

④拒绝服务

最后一种事故类型是拒绝服务(DoS)。通常，这种事故类型是最容易检测的。多的不说了。

G.1 检测（发现）Detection

就是各种入侵检测了，Intrusion detection and prevention system 要做的事，不过要注意判断真假，处理好误报 False-positives 和漏报 False-negatives 问题。

IDS 是旁路带外 out-of-band，IPS 是在线串连 in line。

G.2 响应 Response

许多组织有一个指定的事件响应团队——有时被称为一个计算机事件响应小组(CIRT) computer security incident response team，或计算机安全事件响应小组(CSIRT)。每个单位都有自己的应急响应方案，这没什么好说的。计算机紧急响应团队(Computer Emergency Response Team) CERT，是一个小组，它负责监控，并提出关于安全准备和安全违规的建议。

1.事件响应团队分类

虚拟团队：临时抽组企业内相关专家组成，响应时间较慢，并且其成员在处理事故时必须忽略他们的本职工作，代价很高。

永久团队：专人负责事故响应，对较小的企业来说不适用。

混合团队：个别核心成员是永久性的，而其他成员则在需要时才被召集。

2.过程

许多组织机构都采用三步骤的事故响应过程（其实是 6 个过程合成 3 个了，后面有讲）：

①监测和确认 Detection and identification，确定事故以及通知适当的人员。

②响应和报告 Response and reporting，包括：隔离与抑制、收集证据、分析与报告。

③恢复和补救 Recovery and remediation，修正已发笺破坏，再恢复业务，加固系统。

G.3 缓解 Mitigation

缓解措施尝试遏制一个事件，限制其影响或范围。Mitigation 这个词最好翻译成“消减”。

确定了一项安全事件，响应的第一步就是牵制（Contain it），以控制事件的影响和范围。Containment is the first step after detecting and verifying an incident. This limits the effect or scope of an incident.

G.4 汇报（报告）Reporting

报告是指向组织内部，同时向组织外部报告事件。关于泄密事件，是有法律要求的，一般必须在 24 小时内报告政府。

报告对外发布的对象是由数据所有者决定的。

G.5 恢复 Recovery

调查人员从一个系统收集所有适当的证据后，下一步是恢复系统，或将其恢复到一个完全正常的状态。这个工作量根据事件的影响程度可大可小。不过要考虑病毒、木马等是不是没清干净，要不要彻底的重建系统？

G.6 补救 Remediation

亡羊补牢。在修复阶段（这不是恢复业务的阶段了），人员观察事件并确定什么原因导致它发生，然后实施措施以防止它再次发生。最简单的就是打补丁，最重要的是根本原因分析。

根本原因分析(RCA)/问题管理 Problem management

从根本上说，根本原因分析(RCA)是问“为什么?”，直到有一个答案。RCA 涉及审查系统日志，政策，程序，文档的安全性和捕获网络流量，可以先将小事件拼凑一起以推演出导致的历史事件。一旦该事件被理解，RCA 团队可以反向工作，以确定哪些是允许发生的事件。逆向工作将涉及与事件管理人员和调查人员合作的能力，确保所有相关信息正在被收集，记录和管理，根据组织的事件程序处理，而且监管链是严格保持收集的所有证据。

G.7 汲取经验教训 Lessons Learned

最后是教训总结。事件响应小组将参与这个阶段，但是其它了解该事件的员工也将参与。分析事件的处置流程，总结管理上、技术上、培训上的改进建议。当完成经验教训审查后，通常需要事件响应团队编写一个报告。最烦就是写事件分析报告了。或许，事件响应的最重要的部分是总结经验。组织有机会来分析和理解失败，并尝试以确保它不会再次发生。

这里又要讲一堆的攻击了，都不知道重复多少遍了，再罗列一下：

1.拒绝式服务攻击 Denial-of-Service Attacks

拒绝服务(DoS)攻击能够阻止系统处理或响应来自资源和客体的合法数据或请求。拒绝服务攻击的最常见形式是向服务器传输使其无法全部处理的过多数据包，或让系统崩溃或 100%的 CPU 使用率。另一种形式的 DoS 攻击是一种分布式拒绝服务(DDoS)攻击。还有一种变体的 DoS 形式被称为分布式反射拒绝服务(DRDoS) distributed reflective denial-of-service，域名服务(DNS)投毒攻击和 smurf 攻击就是这样的例子。

2.SYN 泛洪攻击 SYN Flood Attack（让你回不停）

SYN 泛洪攻击是一种常见的 DoS 攻击。它通过破坏 TCP/IP 启动通信会话的三步握手标准来实施攻击。通常，客户端向服务器发出 SYN (同步) 数据包，服务器向客户端发送 SYN/ACK (同步/应答)响应数据包，随后客户端向服务器回应 ACK (应答)数据包。这样三步握手建立起了两个系统间的一个用于数据传输的会话，这个会话直到出现 FIN (结束)或 RST (重置)包才会断开。然而，在一个同步字符(SYN)洪水式攻击发生时，攻击者发送成千上万个 SYN 包但不回复响应。这类似于一个喜欢开玩笑的人伸出手去握手，但是当其他人做出回应，伸出手准备握手时，他却将手缩了回来，留下对方的手悬在半空中。

使用 SYN Cookies 是阻断这攻击的一种方法。这些小记录消耗小部分系统资源，当系统接收到 ACK 应答肘，它检查 SYN Cookie 并建立会话。防火墙通常能够通过入侵检测和入侵防御系统检测 SYN 攻击。阻断这种攻击的另一种方法是降低 TCP 重置攻击服务器通常会等待一段时间以接收 ACK 应答。默认时间是三分钟，但在正常操作中合法系统发送 ACK 应答并不需要这么长的时间。通过减少时间，半开的会话在系统内存中的刷新会更快。

3.TCP 重置攻击 TCP Reset Attack（让你连不上）

另一种通过操纵 TCP 会话的攻击方式叫做 TCP 重置攻击，会话通常是 FIN(完成)或 RST(复位)包。攻击者可以在一个 RST 包中伪造源 IP 地址并断开会话活动。两个系统之间则需要重新建立会话。这对系统来说是一个很大的威胁，两系统之间需要持续的会话，以保持数据。当会话重建时，系统就需要重建数据，所以这不仅仅只是来回发送三个数据包以建立会话的问题。

4.Smurf 和 Fraggle 攻击（前者反弹、后者 UDP）

Srnurf（欺骗）和 Fraggle（磁片）攻击都属于 DoS 攻击。Smurf 攻击是另一种类型的洪水式攻击，但它使用 Internet 控制消息协议(ICMP) 回送数据包而不是 TCP SYN 包攻击其他系统。更具体地说，它是一个使用受害者的 IP 地址作为源 IP 地址的伪造广播 ping，让全网都响应并回送数据包至受害 IP。在 1999 年发行的 RFC 2644 改变了路由器的标准，路由器不能转发定向广播，网络便不能被放大。这给 Smurf 攻击单一的网络带来了限制。此外，在防火墙上禁用 ICMP 能够防止利用 ICMP 的任何类型的攻击。现在 Smurf 攻击已经很少见了。

Fraggle 攻击类似于 Smurf 攻击。然而，Fraggle 攻击使用 UDP 端口 7 和 19 而不是 ICMP。Fraggle 攻击能够使用伪造 IP 地址将一个 UDP 数据包发送给受害者。所有的系统就都会将其转发给受害者，这类似于 Smurf 攻击。

SMURF 是反弹攻击，消耗带宽（ICMP）；FRAGGLE 消耗性能（UDP）。

5.Ping 洪水攻击（呼死你）

Ping 洪水攻击，通过给受害者发送洪水般的请求来达到攻击目的，在 DDOS 攻击中给僵尸

网络发送僵尸信息的效果很明显。如果成千上万的系统同时给一个系统发送 ping 请求，该系统将在试图回答 plng 请求时发生混乱。

6.僵尸网络 Botnets

今天僵尸网络相当普遍。僵尸网络中的计算机就像机器人(通常称为僵尸 zombies，也叫肉机)，并将会按照攻击者的要求执行命令。僵尸牧人 bot herder 通常是指通过一个或多个命令控制所有计算机和服务器的罪犯。

7.死亡之 Ping/Ping of Death（PING 大包）

一个 ping 死亡攻击采用了一个超大的 ping 数据包，即超过 64 字节，甚至大到 64KB。当系统收到 ping 包大于 64 KB 时，就会出现问题。现今死亡 PING 攻击很少能够成功，因为补丁和更新改善了系统的脆弱性。

8.泪滴攻击 Teardrop（拼不完整）

在泪滴攻击中，攻击者阻碍交通，系统无法将数据包一起发回。大数据包通常被分成较小的碎片，当它们被发送到网络上时，接收系统把数据包碎片还原到原来的状态。然而，泪滴以一种系统不能将文件还原在一起的方式分割数据包。旧的系统无法处理这种情况，并会崩溃，但补丁解决了这个问题。此外，入侵检测系统可以检查畸形数据包。

7.Land 攻击（自己搞自己）

Land 攻击是指攻击者使用受害者的 IP 地址作为源 IP 地址和目的 IP 地址，并发送伪造的 SYN 包给受害者。这使系统不断地对自己做出应答，并最终可能会冻结，崩溃或重新启动。这种攻击在 1997 被第一次发现，它又几次攻击不同的端口。保持一个系统更新并使用过滤流量检测相同的源和目的地地址，有助于防止 Land 攻击的发生。

8.零日攻击 Zero-day Exploit

零日漏洞是指利用他人未知的系统漏洞对系统发起攻击，也指无法修补的漏洞。

9.恶意代码 Malicious Code

恶意代码是指在计算机系统上执行不必要的、未经授权的或未知活动的脚本或程序。恶意代码可以采取多种形式，包括病毒，蠕虫，木马，具有破坏性宏的文件，和逻辑炸弹。它通常被称为恶意软件，或恶意代码。恶意代码存在于每一种类型的计算机或计算设备，是现今最常见的安全漏洞。

10.中间人攻击 Man-in-the-Middle Attacks

当一个恶意用户能够在一个正在进行的通信的两个端点之间的逻辑上获得一个位置时，一个中间人攻击就会产生。中间人攻击有两种。一个涉及复制或刺探双方通信，这基本上算是嗅探器攻击；另一种类型是攻击者在通信线上定位自己，他们将其作为一个存储和转发或代理机制，客户端和服务器认为它们是直接连接的。攻击者可以收集登录凭据和其他敏感数据，以及改变两个系统之间交换的消息内容。

中间人攻击比其他许多攻击需要更多技术性，因为从客户角度出发，攻击者需要冒充服务器，从服务器的角度来看，还要模拟客户端。中间人攻击往往需要一个组合的多个攻击。例如攻击者可能会改变路由信息和 DNS 的值，或伪造地址解析协议(ARP)查找。

11.战争拨号 War Dialing

使用调制解调器搜索接受入站连接尝试的系统的行为，就是大量拨号。一旦检测到某个计

算机载波音，战争拨号器就会在搜索过程结束时所生成的报告中添加相应的电话号码。一种新的战争拨号的形式能够在不适用调制解调器的情况下，使用语音互联网协议(VoIP)拨号，这使得攻击者能够扫描到更多的电话号码，并发现除了调制解调器以外的其他设备，如传真机、语音信箱、拨号音和人类的声音。

抵御恶意战争拨号攻击的对策包括：实施强大的远程访问安全性(主要依靠强的身份验证)，确保不存在未授权的调制解调器，以及使用回叫安全机制、协议约束与呼叫登入。

12. 破坏 Sabotage

员工破坏指的是员工对单位的破坏行为。员工被解雇后必须立即终止或禁用其账户，预防员工破坏的其他保障措施还存定期审计、监测异常或未经授权的活动，保持员工和管理人员之间的沟通开放，并适当奖励员工。

13. 间谍 Espionage

间谍活动是一种收集专有的、秘密的、私人的、敏感的或机密信息的恶意行为。

H. 操作和维护预防措施

H.1 防火墙

第四域 B.3 章节已经详细讲过防火墙了。这里不讲了。

H.2 入侵检测和预防系统

入侵检测系统(IDS) intrusion detection system 通过自动检测日志和实时系统事件以检测入侵和系统故障。入侵防御系统(IPS) intrusion prevention system 具有入侵检测系统的所有功能，而且还可以采取额外的措施来阻止或防止入侵。入侵防御系统(IPS)不是旁路接的，是串接在网络的，能够在攻击到达目标系统之前进行检测并阻止攻击。

IDS 的三大基本组件是（采集、分析、告警）：

①传感器/探测器（Sensor），也被称为探针，或代理（Agent），采集数据流量。

②分析器/控制与通讯（Analyzer），收集信息，通过分析确定是否有攻击或滥用行为发生征兆或先兆。

③发声器/用户界面（User Interface），管理员用来查看 IDS 收集的信息以及做出的判断，对 IDS 进行配置和调整所使用的管理界面。

1. 基于知识的和基于行为的检测 Knowledge- and Behavior-based Detection

IDS 通过监控网络流量和检查日志，来检查有无可疑活动。有 2 种常见方法来检测和识别恶意行为：

①基于知识/模式匹配/特征分析（基于规则，经验式的检测）（Knowledge-Based/Pattern matching/Signature-Based）。使用签名，又称基于模式匹配的检测或检测签名。它使用 1 个关于已知攻击的特征的数据库，当模式匹配时，就被认为是一个攻击。它的缺点是，对未知的攻击无能为力。在产品环境中发现的攻击或病毒称为“野生的(in the wild)”。已经存在但尚未公布的攻击或病毒称为“动物园内的(in the zoo)”。（发现的是野生，未知的是园内）

此外，它还包括基于状态匹配(State-Based)的：将某些系统状态转变(State Transition)视为遭受了攻击，以通信流为背景、并分析整个系统的行为，而不是单个数据包或分散的数据报告。状态（State）是操作系统的值在可变的、临时的和永久内存位置上的一个快照。

②基于行为/统计异常（Behavior-based/Anomaly-based/ Statistical Anomaly）。不使用签名，将活动同正常性能的基线进行对比，以检测异常行为。缺点是误报比较多。（基于统计，启发式的检测）

其实比较清晰的分类是这样的：

①基于特征 Signature-based：

包括特征匹配（Pattern matching）和状态匹配（Stateful matching）。

②基于异常 Anomaly-based，也称为基于行为，或启发式：

包括统计异常（Statistical anomaly－based）、协议异常（Protocol anomaly－based）和流量异常（Traffic anomaly－based）。

③基于规则 Rule-based（专家系统），一般把基于规则和基于特征都看成是基于知识的。规则型 IDS 采用一种不同于特征型或统计异常型系统的检测方式。专家系统由知识库、推理引擎和规则型编程组成。知识以规则表示，将要接受分析的数据则称为事实。系统的知识以规则性编程(IF situation THEN action)编写。这些规则应用于事实、来自传感器的数据或者某个被监控的系统。推理引擎负责为这个过程提供某些人工智能；通过使用推理规则，推理引擎可以从提供的数据中推断出新的信息。

也就是说，在专家系统使用的规则型 IDS 中，IDS 从传感器或日志中收集数据，然后推理引擎对这些数据应用预先编程的规则。如果发现与规则相符的特征，那么 IDS 就会发出报警戒提供一个解决方案。

④基于神经网络（Aritificial Neural Network ANN）。专家系统的一种。

2 主机型和网络型的 IDS/ Host- and Network-based IDSs

根据信息来源进行分类，IDS 有 2 种：主机型与网络型。

①主机型 host-based IDS (HIDS)。监视单个计算机系统上的可疑活动，占用系统资源。

②网络型 network-based IDS (NIDS)。监视在网络上进行的可疑活动，对加密数据无效。

NIDS 很难检测交换网络(相对于传统的非交换环境)，因为在这种网络中，数据通过独立的虚拟电路(PVC)传输，而不是像非交换环境那样通过广播传输。IDS 传感器是一个嗅探器，它不能访问这些电路中的所有流量。因此，我们必须从每一个虚拟专用连接中提取所有的数据，复制这些数据，并将数据副本传送到传感器所在的端口(生成端口)。这样，传感器就可以访问进出交换网络的所有数据。

它们的区别和优缺点经常考，不过都很好理解，容易。

3.IDS 响应 IDS Response

当入侵检测系统检测到事件时，也有 2 种响应方式：主动响应和被动响应。在某些情况下，可以在防火墙前后各放置一个被动的检测系统，以检查防火墙的有效性。通过检查两个 IDS 警报，便能确定被防火墙阻挡的攻击类型而不是正在进行的攻击类型。

①被动响应 Passive Response。系统记录事件并发送一个通知。也就是各种形式的告警，怎么处理看着办。

②主动响应 Active Response。系统通过改变环境来阻止活动而不是做记录和发通知。可以使用几种不同的方法来修改环境，如修改 ACLs 以阻止基于端口、协议和源地址的流量输出，甚至禁用某一条通信链路。使用积极响应方式的 IDS，通常被称为 IPS(入侵防御系统)。

4.黑暗网络/暗网/深网 Darknets

对于入侵检测来说，黑暗网络是使用已分配的未使用的 IP 地址和一个检测进入黑暗网络流量的设备，如果一个正在探测网络的攻击者或恶意软件正在试图扩散，那么在黑暗网络中的主机将会探测和捕捉到这个活动。这样的检测很准，很少有误报，因为合法流量不会出现在黑暗网络中。（有点像是蜜罐、蜜网）

对于黑客攻击来说，暗网是不会发现和记录的，隐藏的网络。

H.3 白名单/黑名单

白名单/黑名单很好理解，不解释了，配防火墙都知道。

白名单列表中的电子邮件地址和/或互联网地址，是已知“好”的人。相对应，黑名单列表是已知“坏”的人。灰名单是一种方法，意思是“我不知道你是谁，所以我会通过一些额外的安全措施，使您的电子邮件发出之前，我接受它。”

H.4 第三方安全服务

用第三方要考虑合规性。比如：与第三方公司签订合同，以帮助提供动态应用程序安全测试(DAST)服务，一个 DAST 技术用于检测应用程序有安全漏洞时的运行状态。大多数 DAST 解决方案是基于 Web 的，测试公开的 HTTP 和 HTML Web 启用应用程序。

1.渗透测试 Penetration Testing

渗透测试(通常简称为 pentest)，模仿一个实际攻击来尝试确定攻击者会使用哪些技术绕过应用程序，系统，网络或组织的安全性。它可能包括漏洞扫描，端口扫描，数据包嗅探，DoS 攻击和社会工程技术等。渗透测试的目标有：

①确定系统对于一个攻击的容忍度。（测底线）

②确定员工检测和实时响应攻击的能力。（验能力）

③识别可以降低风险的控制措施。（提建议）

渗透测试和安全评估一样，也有几种不同的类型：

白盒（全知识）、黑盒（零知识）、灰盒（部分知识）。

2.渗透测试的风险

有些方法可能会导致系统或网络中断。

3.道德黑客行为 Ethical Hacking

道德黑客经常被用作渗透测试的另一个名称。道德黑客指的是了解网络安全和并知道如何破解安全性，却不利用该知识为自己谋利的人。就是红客。

H.5 沙箱 Sandboxing

沙箱/沙盒：是一种虚拟化软件，可以让程序运行在自己独立的虚拟环境。它为应用提供了一个安全边界，以防止应用程序与其他应用程序交互，通常情况下，程序运行在沙箱中，对文件和系统限制访问，相关的改变都是临时的。这是一种替代基于签名/特征的防护软件（入侵检测系统）的解决方案，被看作是发现零日，尤其是隐身攻击恶意软件的一种方式，可以检测未知的应用或未知的病毒，也可以用来观察恶意软件的行为。

虚拟机或沙箱有时也称为模拟缓冲区(emulation buffer)。

H.6 蜜罐/蜜网 Honeypots/Honeynets

前面讲入侵检测有一个黑暗网络的技术，其实有点类似了。蜜罐就是用有漏洞的系统或网络来引诱和发现恶意攻击，可以用来延迟入侵者的侵入时间，以便 IDS 尽可能多的检测和收集有关入侵者的信息。蜜罐系统是一个诱饵服务器或系统，通常部署在一个防火墙的 DMZ 区，不能取代传统的安全系统，他们只是标准的入侵检测系统(IDS)的变种，但更侧重于信息收集和欺骗。许多安全专家认为蜜罐能够有效防范零日攻击。这会涉及一些法律问题，当蜜罐的所有者通过“钓鱼执法”来诱捕未授权的入侵者，可能是非法的。

两个或多个蜜罐在网络上形成一个蜜网。通常，**蜜网**是用于监测一个大的/或更多不同的网络，一个蜜罐可能并不够用，也不典型全面。蜜网和蜜罐通常是大规模网络中入侵检侧系统的组成部分。**蜜场**是一个集中的蜜罐分析工具。包括一些常见的蜜罐：

与蜜罐相关的概念还有一个“伪漏洞”Pseudo Flaws。伪漏洞是被故意植入在系统中试图引诱攻击者的虚假漏洞或明显漏洞。

常见的蜜罐工具有：

①Glastopf，开源蜜罐，Python+PHP+MySQL。

②Specter，商业蜜罐。

③Ghost USB，免费的 USB 仿真蜜罐，针对 U 盘病毒。

④KFSensor，基于 Windows 和蜜罐的 IDS。

另一个概念是“**填充单元**/填空模块”Padded Cells。填充单元是一个模拟环境，类似蜜罐一样，通过提供伪造数据来吸引入侵者的兴趣。当入侵者被 IDS 检测到的时候，入侵者被自动地转移到一个填充单元。填充单元具有实际网络的结构和布局，但是在填充单元里，入侵者既不能执行任何恶意的活动，也不能访问任何机密数据。

诱捕(Enticement)为他人的预谋(Ready and Willing)犯罪提供机会。

陷害(Entrapment)是引诱或劝说他人进行非预谋(No Previous Intent)犯罪。

H.7 反恶意软件

阻止恶意代码最重要的措施是使用带有最新文件的反恶意软件的软件 anti-malware。而攻击者则定期发布新的恶意软件，并经常修改现有的恶意软件，以防反恶意软件的检测。反恶意软件厂商寻找这些变化，并开发新的签名文件来检测新的恶意软件并对其进行修改。

1.恶意软件

要监视恶意软件，有必要介绍沙箱和钩子。这些钩子可以直接插入到一个程序去通知或调用(回调函数)库的函数。拦截系统调用的主要问题是，沙箱看不到恶意软件执行任何指令之间的调用。这是一个很大的盲点，恶意软件的作者可以把这个作为一个目标，在系统调用之间运行代码。恶意软件采用了多种技术和方法来逃避检测。这些技术之一将恶意代码延迟执行，使得一个沙箱超时。然而，要做到这一点，恶意软件并不是简单的睡眠。相反，恶意软件执行一些无用的计算活动，恶意软件通过延迟技术的工作原理，因为它在沙箱中仅仅是执行功能，从哪方面来看，都像是一个正常的程序。

另一个逃避的方法是通过环境进行的检查。恶意软件作者可以添加新的，与零日有关的环境，检查相关的系统运行和操作的返回值进行规避，迫使供应商更新他们的沙盘来应对。

I. 实施和支持补丁与漏洞管理

1. 补丁管理 Patch Management

补丁有时被称为更新、快速修复或热修复。服务包是一个补丁的集合，携带着一个系统当前最新的补丁。一个有效的补丁管理程序能够确保系统安装当前最新的补丁。下面是有效的补丁管理程序的通用步骤：

①评估补丁 Evaluate：确定补丁是否适用于他们的系统。

②测试补丁 Test：确定该补丁不会带来其他副作用。

③批准补丁 Approve：确定补丁的安全性后，就会批准补丁的部署。

④部署补丁 Deploy：经过测试和批准，管理员部署补丁。

⑤确认补丁已部署 Verify：在部署补丁后，管理员定期测试和审计系统，以确保系统补丁仍然有效。

补丁星期二和漏洞星期三 Patch Tuesday and Exploit Wednesday。

微软经常在每个月的第二个星期二发布补丁，这一天通常被称为补丁星期二。于是，很多黑客立马利用该补丁所补救的漏洞来进行攻击，因为很多用户不会那么快就把新补丁打上，这个时间段被称为漏洞星期三。

2. 漏洞管理 Vulnerability Management

漏洞管理是指定期检测漏洞，及时修补高危漏洞，评估并采取相应措施以减少相关风险。一个漏洞管理程序的两个常见要素是例行漏洞扫描和定期脆弱性评估。职责分离原则会要求组织中一个人负责补丁，一个人负责漏洞，可以互相验证、监督。

3. 漏洞扫描 Vulnerability Scans

利用漏洞扫描器来检测系统和网络中的漏洞，如补丁丢失或弱口令等，并在被攻击之前修补漏洞。最著名的工具是 Nessus，不过它已经商业化了，要收费。

4. 脆弱性评估 Vulnerability Assessments

从字面上看，就是漏洞水平评估。一个脆弱性评估不只是漏洞扫描结，还要分析过去所有的漏洞扫描报告，以确定该单位是否正在修复漏洞。脆弱性评估往往是风险分析或风险评估的一部分，以确定在一个时间点的漏洞。

短期脆弱性评估有时也被看作是风险评估。做渗透测试的前提也是先做脆弱性评估。

5. 常见漏洞和披露 Common Vulnerabilities and Exposures

主要是官方的漏洞库了。如：通用漏洞披露(CVE) Common Vulnerability and Exposures，它由 MITRE 维护。

J. 参与和理解变更管理流程（例如：版本控制、基线化、安全性影响分析）

变更管理的主要目标是确保变更不会导致中断。变更管理流程要求适当的人员在实施变更前需审查和批准变更，并做详细记录。其实，变更管理的内容放在这个位置不合适，应该在讲完 D.2 章节的配置管理，也就是搞完“基线”后，接着搞“变更”。

1.安全影响分析

做变更，必须先做安全影响分析。变更管理控制提供了一个过程去控制、文档化、跟踪和审计所有系统的变化。在变更管理过程中的常见任务如下：

①请求变更 Request。

②影响分析/影响评估 Impact Assessment

③审查变更 Review

④批准/不批准 Approve/reject/Approval/Disapproval

⑤构建和测试 Build and Test （考试中有排序题，记住要先测试变更，再执行变更）

⑥通知/通告 Notification

⑦实施变更 Schedule and implement。

⑧验证 Validation

⑨记录/版本更新和基线 Document。

2.版本控制 Versioning

如果不能通过某种类型的版本控制系统来控制变更，可能会引发由于变更导致的系统瘫痪。变更管理必须文档化。

K.实施恢复策略

自然灾害有很多，像火灾、地震、洪水、暴雨、台风什么的；人为灾害也有很多，像火灾、恐怖袭击、工业爆炸、停电什么的；此外，公共基础设施的灾害也有很多，像软/硬件故障、停电、罢工、盗窃什么的。信息安全的范畴很大，凡是影响系统和数据安全稳定的因素都要考虑，安全专家必须是全才。

保护服务器、电源什么的是很常见的技术了，不多说。

K.1 备份存储策略（例如异地存储、电子链接、磁带旋转）

这章考的比较细的。

1.磁盘阵列 Redundant Arrays of inexpensive Disks

在计算机中添加容错和系统恢复组件的常见方法是增加一个冗余磁盘阵列(RAID)。一些常见的配置如下：常考是的 0、1、1+0、5。先要了解几个技术：镜像 Mirroring、校验 Parity、条纹/条带化 Striping(字节级、块级的并发存储)。

①RAID-0，也被称为条带 striping。它使用两个或两个以上的磁盘，提高性能，但不容错。写文件到多个磁盘上的条纹上，无奇偶校验信息的使用。这种技术允许快速阅读和写入磁盘，因为所有的磁盘可以并行访问。然而，如果没有奇偶校验信息，不提供冗余，就不可能从硬盘故障中恢复过来。它不能用在高可用性要求的系统上，但它代表了最快的磁盘阵列。

②RAID-1，也被称为镜像 mirroring。它使用两个磁盘，并含有相同的数据信息。如果一个磁盘损坏，另一个磁盘仍含有数据。提供容错。这个级别的所有写入磁盘，并从一个磁盘复制到另一个，创建了两个镜像的驱动器。这种技术也被称为数据镜像。它提供了冗余，当一个硬盘驱动器失败时，另一个是可用的。RAID 1 是非常昂贵的，从驱动器的空间的角度来看，有一半的空间用来做磁盘的镜像了。

③RAID-2，这是理论的 RAID 级别，实际上没有应用，反正很复杂。

④RAID 3 和 4（0 加校验；1 加校验），使用 3 个以上的硬盘，基于 RAID-0 的条带化，增加额外的奇偶校检信息，来实现冗余容错，如果一个数据磁盘失败，还可以重建磁盘的信息。其中，RAID 3 的磁盘空间利用更高，但 RAID 4 的速度更快。在这两种情况下，都有一个硬盘是单独存储奇偶校检信息的，它可能成为速度的瓶颈，也是一个单点故障点。（1 或 0 加上一个校验盘）

⑤RAID-5，也叫做奇偶校验 striping with parity。它使用 3 个或多个磁盘，相当于一个磁盘，其中包含奇偶校验信息。如果单一磁盘损坏，则磁盘阵列将继续运行，但速度会变慢。这一级别需要三个或更多个驱动器来实现，类似于 RAID4，但不使用专用的奇偶校验硬盘，数据和奇偶校验信息是在存在所有驱动器上的。这种阵列是最流行的，可以容忍任何一个驱动器的损失。

⑥RAID 6，使用两组奇偶校验信息，可容忍 2 个硬盘同时故障，并不常用。

⑦RAID-10，也被称为 RAID 1+0、RAID 0+1 或条带镜像 stripe of mirrors。是在条带(RAID-0)配置上再配置两个或者两个以上的镜像(RAID-1)。它使用至少 4 个磁盘，但可以支持更多的，磁盘可添加数应为偶数。即使多个磁盘损坏，只要在每个镜像中至少有一个驱动器继续运行，它就能继续运行。在一般情况下，RAID 1+0 全面优于 RAID 0+1，无论是在速度和冗余。

⑧RAID 15，(镜像奇偶校验集合，即 RAID 1 然后 RAID 5)/(奇偶校验镜像磁盘组，即 RAID 5 然后 RAID1)。这是极端的容错，磁盘空间效率低。

要理解：容错与备份是不同的概念。奇偶检验使用的技术是汉明编码（Hamming Coee）。

RAID 级别	活　动	名　称
0	数据条带化到几个驱动器上，不具有冗余或奇偶校验。如果一个卷出现故障，那么整个卷都无法使用。只用于提高性能	条带化
1	驱动器镜像。数据一次写入两个驱动器。如果一个驱动器发生故障，那么就有另一个驱动器提供完全相同的数据	镜像
2	数据按位条带化到所有驱动器上。使用标识任何错误的汉明码创建奇偶校验数据。这个级别规定可以使用多达 39 个磁盘：32 个用于存储，7 个用于错误恢复数据。如今的生产环境中不使用这个级别	汉明码奇偶校验
3	数据条带化到所有驱动器上，奇偶校验数据保存在一个驱动器上。如果一个驱动器出现故障，那么可以从奇偶校验驱动器重建数据	字节级奇偶校验
4	除了以分组而非字节创建奇偶校验之外，其他方面与级别 3 相同	分组级奇偶校验
5	数据写入到所有驱动器的磁盘扇区单元。奇偶校验也写入所有驱动器，以确保没有单点失败	间插奇偶校验
6	与级别 5 类似，增加了容错功能，它是写入所有驱动器的第二组奇偶校验数据	第二奇偶校验数据(或双奇偶校验)
10	数据同时在几个驱动器上建立镜像和条带，能够支持多个驱动器故障	条带化和镜像

2.独立磁带冗余阵列 RAIT Redundant Array of independent Tapes

磁带媒体也可提供冗余。这被称为独立磁带冗余阵列(RAIT)。一个 RAIT 是机制自动转存和驱动机制之间的磁带设备。RAIT 利用条带，但是没有冗余。这也是常见的使用磁带进行备

份和恢复的多个副本。类似于 RAID，只不过有磁盘变成磁带。

其它的技术还有：

3.大规模非活动磁盘阵列 Massive Array of Inactive Disks (MAID)

是只有处于活动状态的磁盘驱动器才会在某一特定时间内启动的一项存储技术。大规模非活动磁盘阵列在减少电能消耗的同时延长了驱动的使用寿命。

4.数据库恢复 Database Recovery

创建远程数据库内容备份有 3 种主要技术手段：电子链接、远程日志处理和远程镜像。

①电子链接/电子传送 Electronic Vaulting（不是实时同步的/1 天 1 次）

数据库备份通过定时周期性的、批量传送的方式备份到远处的一个场所。如果你使用了电子链接，那么需要记住的是，从宣布灾难开始到数据库准备好当前的数据准备运营，可能存在着相当大的时间延迟。如果你决定启用恢复站点，技术人员需要从电子链接中检索到适当的备份数据，并应用到恢复站点中即将投入使用的生产服务器上。与供应商签订电子链接合同的时候，要考虑存储容量、通信链接带宽、定期测试和在灾难发生时检索到保险库数据所需的时间等各种因素。庞大的数据库是通过其它方式先运输并存储到异地的，再通过链接来访问。

②电子日志/远程日志处理 Remote Journaling（不是实时同步的/1 小时 1 次/更频繁）

远程日志处理是以一种更加迅速的方式完成数据的传输。数据传输仍然是以批量传输的方式进行，但是发生的更加频繁，通常每小时一次或者间隔时间更短。与电子链接不一样的是，在数据库不转移数据文件，只同步日志，备份数据库根据日志自行更新数据。当宣布发生灾难的时候，技术人员找到合适的事务日志并将其应用于生产数据库。

③远程镜像 Remote Mirroring（实时的全备份）

远程镜像是最先进的数据库备份解决方案，也是最贵的。远程镜像所使用的技术水平超过了远程日志处理和电子链接。具体怎么做的，跟日志有什么区别，我不知道。

其实还有其它几种方式：

④磁带传送 tape vaulting

将数据备份到磁带上，然后由一名收发员手动将它们运输到一处异地设施。如果使用自动磁带传送(tape vaulting)技术，数据通过一条串行线路传送到异地设施的备份磁带系统中。维护异地设施的公司对这个系统进行维护，并在必要时更换磁带。在需要时，它可以迅速地备份和检索数据。

5.备份和离站存储 Backups and Offsite Storage

灾难恢复计划(尤其是技术指南) disaster recovery plan 应该完整地说明组织要求的备份策略。有 3 种备份类型：

①完整备份/全备份 Full Backups。

采用离站存储数据，包括全部关键数据。最有效，最费时。

②增量备份 Incremental Backups。

基于最近的完全备份或增量备份，再备份已改变的数据。为了确认文件在上次完全备份后是否有改变，使用归档位（archive bit）标识该文档，即：只复制归档比特被打开、启用或设置为 1 的文件；一旦增量备份完成，所有被复制的文件的归档比特都会被重置、关闭或设置为 0。恢复时，先恢复完全备份，再按时间逐个恢复增量备份。

③差量备份 Differential Backups。/差异备份

基于最近的完全备份，仅备份改变的数据，不改变归档位的值。恢复时，先恢复完全备份，再恢复差量备份。

④差量和增量的区别：一是基础，差量基于上次的完全备份，增量不管上次是什么备份；二是标记，差量不改变归档位，增量改变；三是时间，组合使用完整备份和差异备份，只还原两个备份，更快；组合使用完整备份和增量备份，需要还原最近的完整备份和所有的增量备份，更慢。（差完全、增上次）

不能将差量备份和增量备份混杂起来，这种重叠可能造成文件丢失。

6.驱动器和数据存储

包括存储区域网络(SAN)和网络附加存储(NAS)等。其中最常见的故障类型是驱动器故障。

①SAN 存储区域网络(Storage Area Network)

一个 SAN 包括专用的块级存储和专用的**网络**。包括各类存储设备，如磁带库，光盘驱动器和磁盘阵列。他们利用 iSCSI 协议连接操作系统的本地连接设备，提供了相同的 RAID 水平。SANS 还提供额外的性能，容量和冗余选项等。例如，为温站点或热站点提供系统备件，提供远程异地镜像，等。

②网络附加存储 NAS(network attached storage)

NAS 是一个类似 SAN，但有几个非常重要的区别。NAS 一般设计用于简单存储服务文件，NAS 操作不是块级，而是文件级。常用于 FTP 服务器和其他类型的文件服务器，它们通常映射为网络驱动器。也可以用来提供跨网络的多个系统的存储。它们也普遍支持相同的 RAID 级别，在应用程序和数据库软件平台上，也有额外的冗余选项。例如，数据库同步技术可以使用数据库管理系统在多个位置更新记录。无盘工作站就是通过网络来存储的，就是 NAS，就是**网盘**。

7.磁盘簇

如果所有这一切需要的是基本的数据存储，那么 just-a-bunch-of-drives(JBOD)配置可能是最合适的。如果磁盘配置以这种方式，每个磁盘可以单独使用，并彼此隔离。

在这种情况下，**数据**被存储在离散的磁盘上，而不是存储在多个磁盘上。**分区**通常存储在单个磁盘上(而不是跨越多个磁盘)。在某个驱动程序失败的情况下，所有的数据都会被丢失，但其他驱动器将继续提供。这可能需要使用多个磁盘的一个分区，这称为**级联**。级联磁盘会出现操作系统作为一个单一的连续驱动管理。这可能是最合适的，特别大的分区是可取的，但驱动器故障可能会造成相当大的问题，因为所有的数据在驱动器失败时候将丢失。

K.2 恢复站点策略

1.受信恢复 Trusted Recovery

恢复程序能够保证系统在发生故障或崩溃之后，能够还原因之前的状态。系统可以被预置，在损坏时能够处于**故障防护状态** fail-secure system 或者**应急开放状态** fail-open system。故障防护状态的系统会在故障发生时保持在防护状态，并禁止所有访问；而应急开放状态在发生故障前保持在开放的状态，并允许所有访问。举个栗子就是，一扇自动门如何停电了，是保持关闭还是开放呢？这个选择取决于在系统的业务运行重要还是安全更重要。

失效安全和失效开放 Fail-secure and fail-open

应用程序故障时，其代码应被设计成能有效应对一般意义上的失败，有两个基本选择：

①失效安全状态/故障安全机制：置系统于一个高安全级别(甚至完全关闭禁用它)直到管理员可以诊断问题和恢复系统正常运行。（微软的蓝屏）

②失效开放状态/故障保护控制：允许用户绕过失败的安全控制，忽略错误的发生。

任何系统的恢复过程有两个要素来确保一个可信的解决方案的实施。

一是失败准备。除了备份方案之外，还要有系统恢复及容错的方法。

二是系统恢复的过程。系统应该重新启动，恢复所有受影响的文件和服务，检查所有重要的安全文件的设置等等。

受信恢复有 4 种类型：

①手动式恢复 Manual Recovery

如果系统崩溃了，系统并没有处于故障防护状态。相反的是，在系统故障或崩溃后，管理员需要手动执行必要措施，以实现系统恢复。

②自动式恢复 Automated Recovery（多种故障）

对于至少一种类型的系统故障，系统能够自动执行受信恢复。例如，RAID 硬盘能够恢复硬盘驱动器故障但是不能恢复整个服务器故障。一些类型的故障需要手动恢复。

③无过度损失的自动式恢复 Automated Recovery without Undue Loss

这类似于自动式恢复，对于至少一种类型的系统故障，系统能够自动执行恢复过程。然而，这其中包括一些能够保护特定对象免受损失的机制。无过度损失的自动化恢复的方法包括对数据及其他对象的恢复。它可能含有其他机制，以恢复受损文件，重建日志数据，并验证密钥系统和安全组件的完整性。

④功能恢复 Function Recovery

支持功能恢复的系系能够自动恢复某些特定功能。这种状态能够确保系统成功地完成功能恢复。否则系统将会回到变更前时的故障防护状态。

2.确定业务单元的优先顺序 Business Unit and Functional Priorities

为了尽可能最有效地恢复你的业务运营，你就必须精心策划你的灾难恢复计划，以至于优先级别最高的业务单元能被最先恢复。你必须识别和优化重要业务功能，还有你能定义在发生灾难或错误之后你想恢复哪个功能或者以什么顺序恢复。

第一域的 G.2 章节已经讲过业务影响分析 BIA 了，这里也要用到。大多数单位将 BIA 作为业务连续性规划过程的一部分，这种分析能够检测漏洞、建立策略来降低风险， 并最终生成一个 BIA 报告以描述组织面临的潜在风险并确定重要的商业单元和功能。拥有所有的 BIA 信息，便可以使用生成的文件作为优先级任务的基础。

3.可替代的工作站点 Alternate Processing Sites

灾难恢复计划中最重要的要素之一是：在主要的工作站点无法使用的时候，选择可以替代的工作站点。在灾难恢复计划中经常使用的几类站点有：冷站点、温站点、热站点、移动站点、服务局（service bureaus）以及多站点。

热站是在线的，其它都是离线的离站。Offsite。

①冗余站点（rddundant site）冗余场所/镜像站点

地理上分散的两个数据中心，之间热交换或负载平衡，可以完全接替，连人都有备份。

冗余中心的优势：*很少或没有停机时间、*易于维护、*没有恢复需求

冗余中心的缺点：*更多的费用、*需要冗余的硬件、网络系统和员工、*距离限制

②内部或者外部热站点（hot site）/完备场所

内部热站点：该站点是准备就绪的，包括所有的技术、设备和应用程序，有实时数据。

外部热站点：与服务商提供签约提供的，与在线站点尽可能接近。在外部热站点上只有硬件，没有任何应用程序或数据。

内部或外部热站点的优点：*允许测试恢复、*高可用性、*站点快速恢复

内部或外部热站点的缺点：*价格昂贵、*外部站点的硬件和软件兼容性问题

③温站点或冷站点（warm site/cold site）基本完备场所/基础场所

温站点：有基础设施(空调/电脑/布线/通信)，无服务器、无数据（通常 12 小时启用）。

冷站点：空的数据中心空间，只有物理设施，所有设备和技术必须在灾难时购买或获得。

温和冷的网站的优点：*更少的费用、*长期恢复的可用性

温和冷的网站的缺点：*不能立即使用、*没有完整的测试、*只支持部分关键业务恢复

④移动站点（rolling hot site）滚动完备场所

将数据中心被安置在一个移动拖车或一个标准的海运集装箱中。灾难发生时，将它移动到另一个有必要的电力、资源和通信的地点继续经营。

移动站点的优势包括：*高可移动性、*模块化、*不需要房间

缺点包括：*冷站点能力有限、*密度和容积升级容量有限、*运输成本高

⑤互助协议/互惠协议 Mutual Assistance Agreements/ reciprocal agreement

互惠协议（reciprocal agreement）是在组织之间分担彼此风险，帮助对方在空难中恢复数据和处理。虽然合乎逻辑，但也充满兼容性、竞争保密、性能不足等问题。

联盟是互惠协议的一个变体，也称为相互援助协议（mutual aid agreement），就是多个组织互相帮助。

⑥服务局 Service Bureaus（相当于云服务供应商或产品租赁商）

服务局是租借计算机时间的公司。服务局拥有很大的服务器群，并且通常具有大量工作站。任何组织机构都可以与服务局签署购买合同，以便使用部分处理能力。访问可以是联机的，也可以是远程的。在发生灾难时，服务局的工作人员通常能够为你的所有 IT 需求提供支持，甚至工作人员还能够使用台式机。与服务局签署的合同往往包含测试和备份以及响应时间和可用性。

⑦外包

为了避免这些问题的互惠协议和建设替代站点的成本，一些组织可以通过服务水平协议(SLA)选择外包他们的应急行动和灾难恢复。但真出事了，不一定靠谱。

4.集群

集群技术也可以使用，但不是冗余和负载平衡。在集群技术中，双活系统可以随时提供服务，在一个系统失败的情况下，会降低服务能力。

K.3 多处理站点（例如：运行的冗余系统）（multiple processing center）多处理中心

企业的另一种备份方案，如跨国公司在世界各地都有服务站点，就可以互为备份。这是新

加的内容，不知道怎么考。

K.4 系统弹性、高可用性、服务质量和容错

系统的弹性、高可用性、服务质量和容错的备件冗余项目被称为在系统中提供容错。就是容灾备份了。总之：冗余、容错和故障转移功能提高了系统或网络的可靠性；高可靠性可实现高可用性。

1.容错能力 Fault Tolerance

是指系统在发生故障的情况下，仍然继续运行的能力。容错性是通过添加冗余组件实现的，如在廉价冗余磁盘阵列(RAID)中的额外磁盘，或在故障转移群集配置中的额外服务器。

2.系统弹性 System Resilience

指的是系统在发生不利事件时保持一个可接受的服务水平能力。这可能是硬件错误，或可能是其他控制管理的攻击。在某些情况下，它指的是在发生不利事件后，系统的还原能力。

容错能够使得系统故障转移到另外的服务器上，而系统弹性能够保障在原系统修复后，该集群能够返回原服务器。

3.服务质量 Quality of Service

服务质量（QOS）控制能够保护负载下的数据网络的完整性。许多不同的因素有助于提升最终用户体验的质量，服务质量对这些要素进行管理，以创造能够满足商业需求的环境。有助于服务质量提升的一些因素如下：

①宽带 Bandwidth——可供通信的网络容量。

②延迟 Latency——时间数据包从源到目的地所需要的时间。

③抖动 Jitter——不同数据包之间的延迟变化。

④丢包 Packet Loss——数据包可能会在源和目的地之间的传送过程中丢失，需要重传。

⑤干扰 Interference——电噪声、故障设备等因素可能会损坏数据包的内容。

除了控制这些因素之外，QOS 也会给业务按优先级排序，先保障高级别的业务。

4.高可用性(HA)

高可用性(HA)是保证一些业务始终正常运行的一种技术和流程的结合。具体业务可能是一个数据库、一个网络、一个应用程序、一个电源等。服务提供商与他们的客户之间有服务水平协议 SLA，其中概述了它们承诺提供的正常运行时间和当网络无法连接时能够使该服务正常运转的周转时间。例如，托管公司可以保证互联网连接提供 98%的正常运行时间。这意味着它们可以保证至少 98%的时间内你在他们那儿购买的互联网连接能够正常启动并运行。为了提供这种级别的高可用性，托管公司需要有提供冗余、容错和故障转移的技术与过程。

L.实施灾难恢复流程

要实施灾难恢复，先要拟制好灾难恢复计划。怎么写，怎么分发和维持就不说了。

L.1 响应 Emergency Response

灾难恢复计划中包含重要人员在识别出灾难或灾难即将来临时应立即遵守的、简单但内容全面的指令，还有各种时限要求。要先重点、后一般的按优先级来处置。

L.2 人员 Personnel

发生灾难，首先要评估其破坏与影响，然后立马查看通知清单，通知所有相关的人员立即处置。有几个小组各司其职：执行应急管理团队、应急管理小组、灾难恢复小组等。

其中：**重建团队**(restoration team)负责使备用站点投入运行，而**救援团队**(salvage team)负责恢复原始站点业务。两个团队必须了解如何完成许多工作，如安装操作系统、配置工作站和服务器、布置电线和线缆、建立网络和配置网络互联服务、安装设备和应用程序。这两个团队还必须知道如何在备份设施中恢复数据，以及如何安全地完成各份工作，保证系统和数据的机密性、完整性和可用性不会遭到破坏。

L.3 通信 Communications

事件的实时态势需要及时通报到各部门、各层级。

L.4 评估 Assessment

当灾难恢复团队到达现场时，他们的首要任务之一就是评估现状。这通常以迭代的方式进行：第一响应者进行非常简单的评估、分类活动并启动灾难响应。随着事件的发展，更加详细的评估将去衡量灾难恢复工作的有效性以及资源分配的优先级。一般会先评估确定：

①非事件：这些事件通常是由系统故障或人为错误导致的服务微小或有限中断。一个短周期的停机时间和不需要备用处理或存储设施。

②事件：导致整个设施或无效的大量时间服务中断的事件。这些事件需要制定灾难恢复计划，并向高级管理层报告信息和状态，并可能需要启用危机管理。

③严重事件：一个关于组织使命，设施和人员的重大破坏或中断：这些事件需要制定的DR.计划，并可能涉及建设一个新的主要设施。这些事件需要高级管理层报告并启动危机管理。

L.5 恢复

要区分清楚什么是灾难**恢复**，什么是灾难**还原**！Recovery vs. Restoration

发生灾难时：**恢复**是将业务操作和过程还原至工作状态；一支灾难恢复团队被指派恢复主要业务，在通信领域就是“先代通，后抢修”；灾难恢复团队成员可以操作的时间范围很短，他们必须尽可能迅速地应用 DRP 和还原 IT 能力。如果灾难恢复团队不能在 MTD/RTO 内还原业务过程，那么公司就会遭受损失。**还原**是将业务设施和环境还原至可工作状态。一旦人们相信原有场所是安全的，那么抢救团队成员就会开始工作，将公司还原至其最初的全部能力，并且在必要时还原至原始位置。如果原始位置不再存在，那么就需要为公司选择新的地点并还原。在通信领域就是“抢修后，再还原”。只有在全部的正常操作都返回至被还原的原有场所后，我们才能宣告紧急状态结束。恢复发生在 RTO 时间，还原发生在 WRT 时间。

L.6 培训与意识 Training, Awareness

培训和文档记录都很重要。别的没什么了。

M. 测试灾难恢复计划

有灾难恢复计划 DRP 还不够，必须定期进行测试，测试和灾难恢复演练应当至少每年进行一次，以确保计划的是可行的并且符合组织机构变化的需要。测试最重要的目的是让人员熟悉

恢复流程和操作，其次才是验证计划本身。

一般有 5 五种主要的测试类型：通读测试、结构化演练、模拟测试、并行测试和完全中断测试。就是后面的 M.1 到 M.5 的内容。先了解几个概念：

灾难恢复（DR）Disaster Recovery，从紧急状态恢复服务的过程，目的就是恢复业务。

灾难恢复计划（DRP），是应对突发情况的应急实施计划，关注 IT 和技术问题。

连续性计划（BC）Continuity Plan，提供方法和程序以面对长期的中断和灾难。

业务连续性计划（BCP）Business Continuity Plan，包含 DRP，内容更广泛。这个内容不在本域，更关注管理方面、流程方面。详见第一域 G 章节。

业务连续性管理（BCM），包含 DRP 和 BCP，提供一个框架，实施管理，形成能力。

有关各种时间的概念，详见 K 和 N 章节。

M.1 核对性测试/检查性测试/通读测试 Read-Through Test/Checklist

通读测试是一种最简单的测试，但也是最重要的一种测试。你只需向灾难恢复团队的成员分发灾难恢复清单的副本，并要求他们审查清单。这样就允许你同时实现下列三个目标：

①恢复清单确保关键人员意识到他们的职责并定期了解掌握相关知识。

②恢复清单促进人员审查过时的信息，并根据组织机构的变化更新相关条目。

③恢复清单能够帮助标识要离职的重要人物，并作出相应的调整。

各自查文档。

M.2 演练性测试/结构化检查/走查 Structured Walk-Through

结构化演练也被称为“桌面练习/桌面演练”table-top exercise/ Tabletop Exercise/Structured Walk-Through Test，简单、成本低。灾难恢复团队的成员聚集在一间大会议室中，不同的人在灾难发生时扮演不同角色。通常，确切的灾难情景只有主考员知道，他在会议上向团队成员描述具体的情况。然后，团队成员通过参考他们的灾难恢复计划对特定的灾难类型进行讨论，进而得出适当的响应办法。

集中推流程。

M.3 模拟测试 Simulation Test

模拟测试与组织演练类似(或战争游戏)，也叫排演演练 Walk-Through Drill。相关人员都集中起来，在特定的模拟环境（场景）中演练灾难恢复，还能提高人员的安全意识。消防演习是一种常见的模拟测试。模拟测试为灾难恢复团队的成员呈现一个情景并要求他们产生出适当的响应措施。与前面讨论的测试不同，其中某些响应措施随后会被测试。这种测试可能涉及到中断非关键的业务活动并使用某些操作人员。

模拟环境搞演练。

M.4 并行测试 Parallel Test

并行测试，也被称为功能测试 Functional drill，利用测试窗口时间在实际的异地备份站实施实施运行测试，还不能影响业务运营。备份站点的处理结果要与原站点的处理结果进行

比较，一般商业服务合同包括每年至少有一个星期用于测试。并行测试涉及到将实际人员重新部署到替换的恢复场所和实现场所启用措施、被重新部署到该场所的员工、以灾难实际发生时的方式执行他们的灾难恢复职责。唯一的差别在于主要设施的运营不会被中断，这个场所仍然处理组织机构的日常业务。

不影响业务，另行做测试。

M.5 完全中断测试 Full-Interruption Test

完全中断也称全面测试 Full-ScaleTest，是成本最高、最复杂的测试。实际站点和业务全部关闭，要求备份站点和恢复过程必须满足准确性、完整性，恢复团队和人员必须具备相应能力。一般只有在成功进行平行测试，前有督导委员会和高级管理层的授权下进行。完全中断测试与并行测试的操作方式类似，但涉及到实际关闭主场所的运营并将其转移到恢复场所。出于很明显的原因，完全中断测试安排起来极其困难，并且你经常会遇到来自管理层的阻挠。

真实系统上的演练。

N. 参与业务连续性计划和演练

建立和维护业务连续性计划（BCP）的最关键部分是管理层的支持。

先复习几个重要时间概念（必考）：

MTD/MTO（最大容忍故障时间 Maximum Tolerable Degradation），时间一到，业务完蛋。

RTO（恢复时间目标 recovery time objective），要采取措施，在领导要求的时间内、在业务瘫痪前搞定故障，恢复系统。【MTO=RTO+WRT，或 MTO-RTO=WRT】

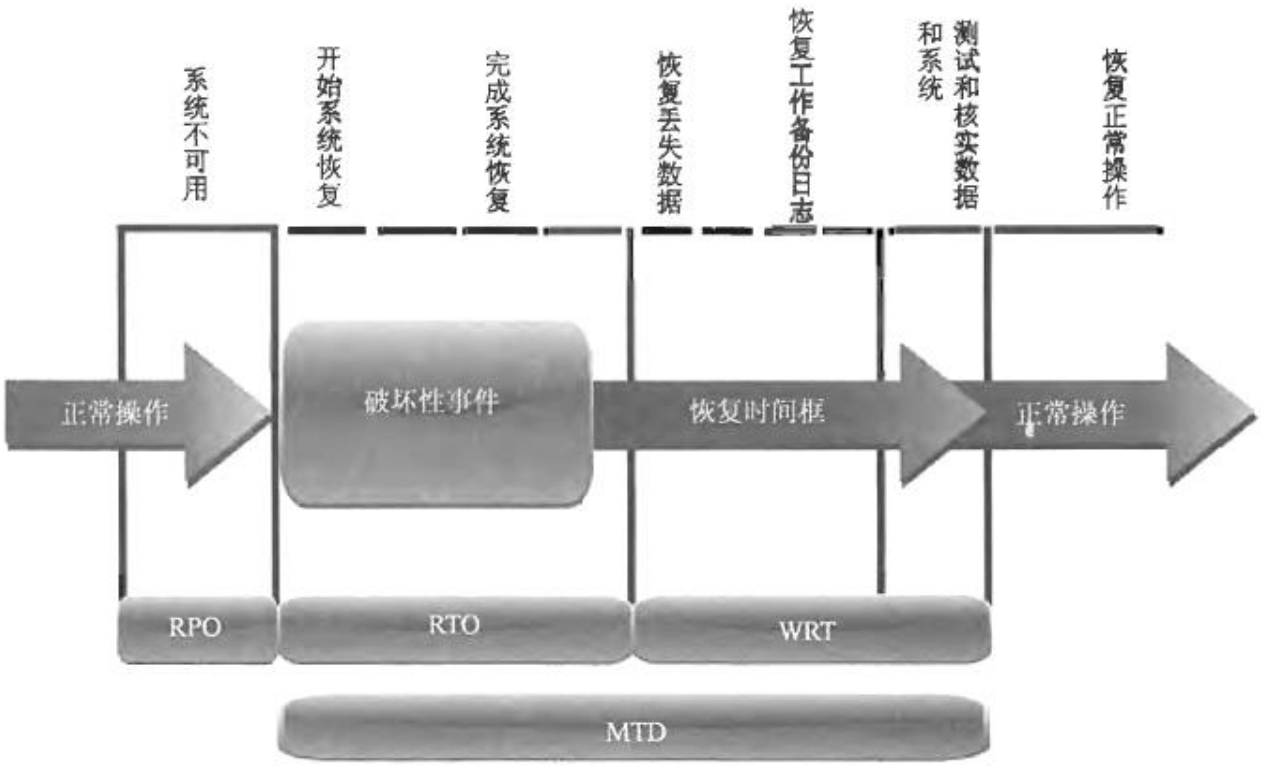
WRT（工作恢复时间 Work Recovery Time），是整个 MTD 值减去 RTO 的剩余时间，是系统和技术恢复后，对人员、业务、数据等进行恢复。RTO 通常指使基础设施和系统恢复运行的时间，而 WRT 指恢复数据、测试流程以及使所有事情“活“过来可以进行生产的时间。

RPO（恢复点目标），可容忍的最大数据丢失量，用中断的最大时间表示，一般都不长。比如某系统的 RPO 是 5 分钟，持续丢失超过 5 分钟的数据量，业务就完蛋了。

MTBF（平均故障间隔时间，Mean Time between failure），代表了设备稳定运行的寿命，是指某一台设备的估计寿命，时间到就该换设备了。

MTTR（平均修复时间，to repair），维修恢复故障设备的时间。

灾难恢复的各类时间标准以及运用方法和意义如下图：



1.NIST 800-34 中的业务连续性规划的流程

业务连续性规划中的业务影响分析 BIA 是很重要的内容，在第一域的 G.2 章节已经详述了相关流程。

NIST800-34 文档是专门针对 IT 的应急计划，当然，它也同样适用于制定企业级的 BCP 和 BCM。所有的团队成员都有义务参加变更控制程序。评审应按 BCP/DRP 策略进行，一般每 3 个月组织 1 次审查，每年进行 1 次正式审核，或者有任何重大的组织改变的时候。

①制定业务连续性规划策略声明。——连续性策略，为计划和建立 BCP 的工作提供了框架和管理，包括：范围、任务、原则、指南和标准。

②进行业务影响分析（BIA）。——业务影响分析，包括风险评估和资产赋值，流程为：搞数据收集、定关键业务、定依赖资源、算资源寿命、定漏洞威胁、算业务风险、写分析报告。

③制定预防性控制方法。——控制措施

④制定恢复战略。——恢复战略

⑤制订应急计划。——制定 BCP

⑥测试计划及进行培训和演练。——测试和演练

⑦维护计划。——维护计划

项目的单个目标必须进行分析，证明计划是有用可行的，确保每一个目标是能够实现的。即 **SWOT 分析**，其基本元素包括：

*优势 Strengths——项目团队的特点，使其比其他团队具有更大的优势。

*劣势 Weaknesses——相对于其他团队，使该团队处于不利地位的特征。

*机会 Opportunities——可以促进项目成功的元素。

*威胁 Threats——可能促使项目失败的元素。

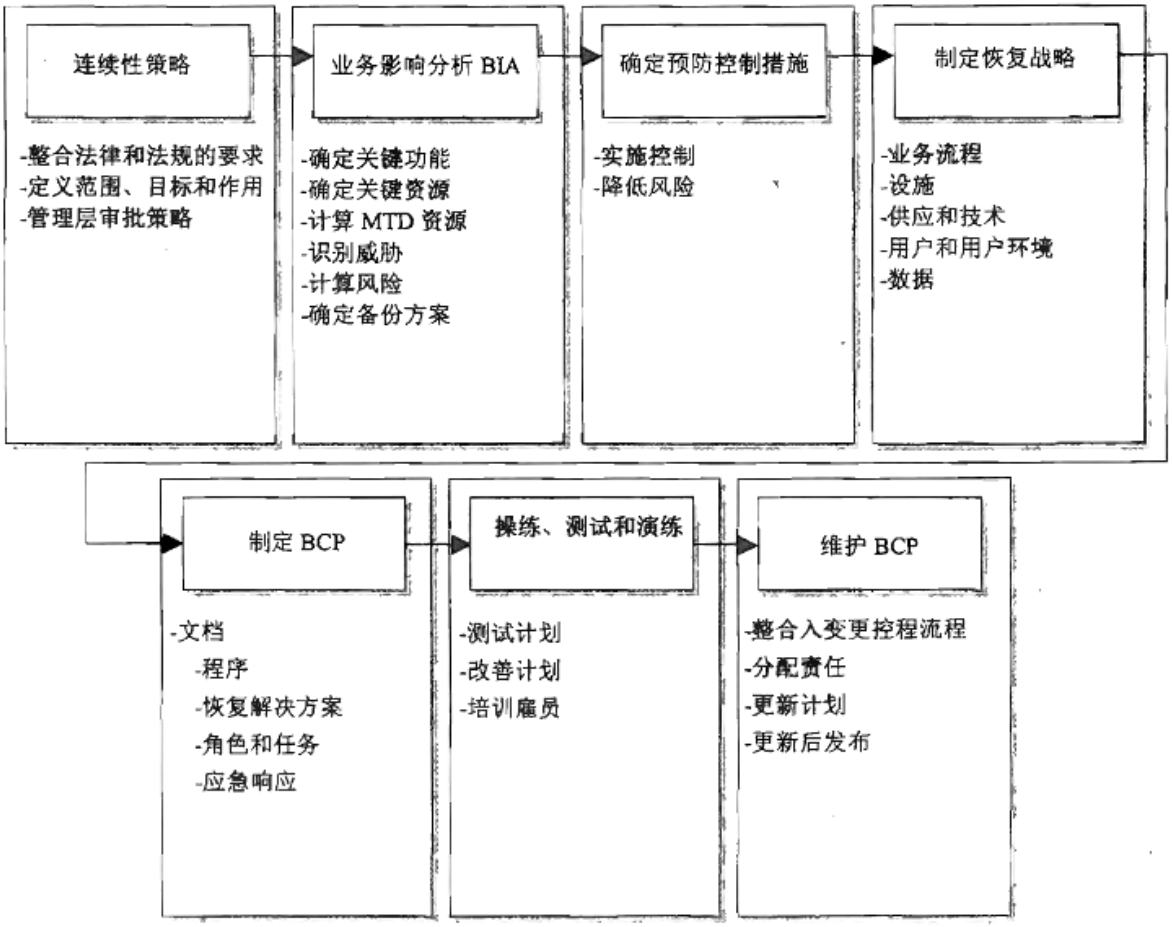


图 8-4　制定业务连续性规划的步骤

2. 业务连续性规划

业务连续性规划项目是一个持续的过程，是指本程序的所有任务都需要定期重复，以确保计划在公司的组织和技术环境下保持当前的现状。其方案提供了在业务中断、组织瘫痪的情况下，公司的关键职能如何延续。

3. 应急管理组织(EMO)/BCP 委员会

EMO 是提供正式的响应过程的管理和现场汇报的团队，用来应对大规模突发事件和提供技术支持。

4. 参与和演练

BCP 的计划工作组开发、实施、并维护公司全部的应急计划。该工作组负责领导和指导相关行动，协助管理层在组织中断的情况下，实施应急处置和及时恢复。

关键人员有：

①BCP 经理：创建计划，负责进行业务影响分析和风险评估。

②BCP 协调员：开发、维护、实施业务连续性和灾难恢复方案与策略，懂项目管理。

③BCP 部门：制定战略恢复计划和连续性计划，并呈审报批。

5. 业务连续性计划员

业务连续性计划员是公司的一个联络点，涉及应急计划或应急反应，为了减少混乱、提高通信效率，实现及时延/恢复组织的整合。

6. 关于 BCM 的其它国际标准

①BS 25999

英国标准协会(BSI)的业务连续性管理(BCM)标准。BS 标准有两个部分：

*25999-1：2006 BCM 业务守则，提供过程、原则、术语体系，即提供业务连续性管理的相应过程、原则和术语体系的一般指南。

*25999-2：2006 BCM 规范，说明执行目标及审核需求，即细说明执行、运作和增强一个 BCM 系统的目标以及审核需求。

②ISO/IEC27031：2011 业务连续性的 ICT(信息和通信技术)准备指南。

此标准是 ISO/IEC27000 整个系列标准的一个组成部分。

③ISO 22301

业务连续性管理体系的国际标准，取代 BS-25999-2。

④GPG（业务连续性协会的优秀实践指南）

BCM 的最佳实践，分为管理实践和技术实践：

*管理实践方面：策略和程序管理；在组织文化中嵌入 BCM。

*技术实践方面：理解组织；确定 BCM 战略；制定和实施 BCM 响应；演练、维护和修订。

⑤DRI 国际协议的业务连续性规划人员专业实践

将业务连续性管理流程分解为以下 10 个部分：

*项目启动和管理。　　*风险评估和控制。

*业务影响分析。　　*业务连续性战略

*应急响应和运作。　　*业务连续性规划

*宣传和培训计划。　　*业务持续计划演练、审核和维护

*危机沟通。　　*与外部代理机构的协调

0. 实施和管理物理安全

相关内容看第三域的 K 章节，前面讲的是怎么选址、建楼什么的，这里就讲怎么保护楼。

0.1 周边安全（例如：访问控制和监控）

1. 周边/物理的访问控制 Perimeter

在控制对某区域的授权访问时，最常见的一个问题是“混入(piggybacking)”，也就是一个人通过使用其他人的合法凭证或访问权利来获取未授权访问。

①屏障/隔离 Barriers

包括自然的和人工的，用于阻碍而或延迟访问；可以隔开入侵者、阻碍入侵者并使得入侵者保持一段距离。

②栅栏/围栏 fence

栅栏 fence 是外围设备，包括地上的划线、铁丝网、带刺铁丝网、水泥墙和使用激光、运动探测仪或热源探测仪的不可见防线等。

3 到 4 英尺高的栅栏可以阻挡**偶然**的侵犯；

6 到 7 英尺高的栅栏难以攀越，可以阻止**大多数**入侵者。

8 英尺或更高的栅栏（带有 3 股带刺铁丝网）可以阻挡信心**坚定**的入侵者（用于监狱）。

▲丝号和网眼（gauge & mesh）

栅栏金属丝的丝号是指栅栏网眼所使用的金属丝的粗细程度。丝号越小，金属丝的直径越

大。11 丝号=0.0907 英寸直径；9 丝号=0.1144 英寸直径；6 丝号=0.162 英寸直径。

网眼大小是金属丝之间的最小净距离。一般的网眼大小为 2 英寸、1 英寸和 0.375 英寸。

金属丝越粗，栅栏越难剪断；网眼越小，栅栏越难以爬过或剪断。反正都是数值最小，强度越大，而且是搭配使用（网眼特别小里，铁丝就没办法粗）。

以下是当前链环栅栏常用的丝号和网眼大小：

*安全性极高——0.375 英寸网眼、11 丝号。

*安全性非常高——1 英寸网眼、9 丝号。

*安全性高——1 英寸网眼、11 丝号。

*安全性较高——2 英寸网眼、6 丝号。

*普通行业安全性——2 英寸网眼、9 丝号。

③十字转门/旋转门 turnstile

每次只可以进一个人，并且只能单向转动，车站经常有这样的门，只出不进。

④陷井/陷门 mantrap

由保安人员守护的双重门，目的是为了牵制主体，直至其身份得到确认和验证。银行里这种门挺多的。还有门 gate 和墙壁 walls 就不说了。

大门一般分为以下 4 类：

• Ⅰ类住宅用途。

• Ⅱ类商业用途。允许普通大众访问，如公共停车场入口大门、社区大门或私人存储间门。

•Ⅲ类工业用途。限制人员访问，如库房大门就不允许普通大众通行。

•Ⅳ类禁止访问。例如由警卫或电网保护的监狱入口大门。

⑤PIDAS 栅栏

边界入侵检测和评估系统 PIDAS (perimeter Intrusion Detection and Assessment)是一种栅栏，其线网上和栅栏底部装有传感器。PIDAS 用于检测入侵者剪断或攀爬栅栏的企图。如果检测到入侵行为，那么传感器会发出报警。PIDAS 非常敏感，经常会导致误报。

2.照明 Lighting

要让敌明我暗，但不能扰民。美国国家标准和技术研究院(NIST)制定的使用照明的边界保护标准中规定了关键区域应该是 QQEE 的被照亮区域、也规定了灯柱的间距应当与照明区域的直径相等。也就是说，如果照亮区域的直径为 40 英尺，那么灯柱的间距同样应当为 40 英尺（无死角）。

室内亮度标准：5-10 fc；

室外亮度标准：大楼入口 Building entrances：5 fc；走廊 Walkways：1.5 fc；停车场 Parking garages ：5 fc；建筑外观 ite landscape 0.5 fc；建筑周边 Areas immediately surrounding the building：1 fc；公路 Roadways：0.5 fc。

室内 5 到 10，室外全是 5 以下。

0.2 内部安全（例如： 陪同要求/参观人员控制、钥匙和锁）

1.内部安全 Internal Security

①锁 Locks

通常在设施的不同区域使用不同形式的钥匙或密码锁。比如：在公用出入口使用钥匙和钥匙卡；在员工各自独用的入口(如存储柜、文件柜等)使用密码锁。宾馆、高档小区、机关都已经使用可编程的门禁系统了，或电子访问控制锁 EAC（electronic access control）。

锁的强度分为 3 级（门的 I 类最差，锁的 1 级最好）：

•1 级商业和工业用途。

•2 级重要的住宅区/次要的商业区。

•3 级居民/消费者消耗物。

锁的类型：

•机械锁。机械锁主要分为两类：暗锁和弹簧锁。

暗锁(warded lock)是最基本的挂锁，它具有一个中间插有凹槽的弹簧锁簧，是价格最低廉的锁，因为它们非常简单，而且很容易被撬开。（锁芯没有弹簧，只有齿凸）

弹簧锁(tumbler lock)的零件更多一些，钥匙插入锁芯，将锁中的金属条推升至正确的高度,让锁簧滑动到锁定或开锁位置。(弹子锁,最常见的)。弹簧锁也分 3 类:销簧锁(pin tumbler lock)、盘簧锁(wafer tumbler lock，也称为晶圆门锁(disc tumbler lock))和杆锁

•组合锁(combination lock)。需要正确的数字组合开锁（转动轮子）。

•密码锁(cipher lock，也称为可编程锁)没有钥匙，它使用数字键盘。密码锁的性能提升有 4 种方法：

*开门延迟时间。如果门长时间打开，将触发一个报警器，以警示可能有可疑活动。

*密码重置。可以编程的特定号码组合，在紧急情况下用于重置密码。

*万能钥匙。使管理人员能够改变开锁密码。

*被困报警。如果一个人被困在锁外面，他可以通过某个号码组合与保安或警察联系。

②员工证/胸牌 Badges

员工证、身份证或安全 ID 都是物理身份标识和/或电子访问控制设备的形式。员工证提供身份验证和授权，通常包括照片、带有编码数据的磁条和个人信息。

③运动探测仪 Motion Detectors

有很多种：

*infrared 红外运动探测仪，对被监控区域红外照明模式的显著变化进行监视。

*heat-based 热能型运动探测仪,对被监控区域中的热能等级和模式的显著变化进行监视。

*wave pattern 波形运动探测仪，向被监控的区域发射连续的弱超声波或高频微波，并且对反射波的显著扰动或变化进行监视。

*capacitance 电容运动探测仪，对被监控物体周围区域的电场或磁场变化进行探测。

*photoelectric 光电运动探测仪，通常在没有窗户或保持昏暗的房间内部使用。

*passive audio 无源音频运动探测仪，对被监控区域中的非正常声音进行侦听。

*Microwave 微波探测：有 3 种

=>bistatic and monostatic 双基或单基：将受控的微波能量的辐射进入保护区，发射的微波信号被收到并建立“没有入侵”的基本水平；

=>bistatic sensor 分离式传感器：在发送器和接收器之间发送不可见容量的微波；

=>Monostatic microwave sensors 集成式传感：集成发送和接收能力的单个探测单元。

④入侵警报 Intrusion Alarms

也有很多种：

*威慑报警 Deterrent Alarms。采用加锁、关门等措施使得进一步的入侵或攻击变得更难。

*排斥报警 Repellant Alarms。汽笛或钟声，还有灯，令入侵者气馁并且离开这个设施。

*通知报警 Notification Alarms。不警示入侵者，仅记录事故数据，并且通知管理员、保安和执法机构。

*本地报警 Local Alarm System。就是本地的。

*集中式警报系统 Central Station System。通过到远程或集中式监控站。大多数中央集中式系统都是知名公司，如 Brinks 和 ADT。

*辅助警报系统 Auxiliary Station。辅助警报系统可以加入本地或集中式警报系统中。当安全边界被侵入破坏时，紧急服务将被通知对事件作出反应并传送到相应地点。这些地点可能包括消防、警察和医疗机构

⑤闭路电视/视频监控 CCTV(Closed Circuit TV)

CCTV 需要人员观看所捕获的视频来检测可疑和恶意的活动，当然它也有自动识别功能。一般是作为二次或后续的监控机制，对可疑情况进行审查。CCTV 既是一个预防措施，在审查记录事件时也是一个检测措施。CCTV 有 4 个基本部件：摄像头 Camera、传输介质 Transmission media、监视器 monitor、外设 Peripherals。

考试会涉及到不同场景需要选择不同的摄像头、镜头、焦距、景深、光圈等等，具体标准自己根据经验猜吧，懒得摘录了。

景深 The depth of field：

镜头打开越小，景深越大；拍摄目标越远，景深越大；焦距越小，景深越大。

⑥二次验证 Secondary Verifi cation

员工经常也会有误操作，那么多监控系统也会有误报，这就需要二次验证（输入 2 次密码）。

P. 参与解决人员安全问题（例如胁迫、旅行、监控）

1. 旅行

旅行外出必须要注意安全保密。如：不带无用的设备，创建强密码，加密敏感信息等。

2. 胁迫

就是被威胁时，怎么处置。讲不清楚。

第八域　软件开发安全（理解、应用与执行软件安全）

Chapters 20,21 in OSG 7th

Chapters 10 in AIO 6th

A.理解安全并将其应用于软件开发生命周期

以前旧大纲操作系统安全里的部分内容合到软件开发安全里来了。

一、基础知识

1.编程语言 Programming Languages

①第一代语言(1GL)机器语言 machine languages。CPU 直接执行的指令。（16/2 进制）

②第二代语言(2GL)汇编语言 assembly languages。用符号来代表机器指令。

③第三代语言(3GL)编译语言（高级语言）compiled languages。用单词语义作为命令。

④第四代语言(4GL)非常高级语言 Very High-Level。类似自然语言，面向问题，只要说“做什么”不用写“怎么做”，包括数据库使用的 SQL。

⑤第五代语言(5GL)自然语言/知识库语言/人工智能语言，允许编程人员创建使用可视接口的代码，目前还没出现。natural languages/Visual interfaces

此外，其他语言(例如 JavaScript 和 VBScript)是解释性语言，即脚本语言。系统使用解释器来执行这些源代码，而不需要源代码编译为可执行文件。

2.编译方法

①汇编程序 assemblers。将汇编语言源代码转换成机器语言。

②编译器 compilers。将高级语言转换成处理器能理解的机器级别格式的语言(exe/dll)。编译器可将高级语言编写的软件源代码编译成适合各种平台的可执行程序。

③翻译器/工具解释器 interpreters。不编译生成可执行文件，而是在执行过程中将高级语言翻译成机器指令，直接运行。最大的优点是支持跨平台并且翻译器有内存管理的功能，缺点是不能独立运行，需要安全本地的翻译器（运行环境），如 JVM、.NET。

④碎片回收器/垃圾回收(garbage collector)。识别并回收之前被使用但已不再被调用的内存块，同样也收集空闲内存的散块(scattered blocks of free memory)并将这些散块组合成更大的内存块。所谓的垃圾回收机制。

3.面向对象编程 Object-Oriented Programming

搞清楚“类/class”和“对象/object”就行了，只要编过程序，这都不难。

较早的编程风格(例如函数式编程)关注程序流本身，是信息流模型（输入=>处理=>输出）。面向对象的编程关注的是对象，更适合建模或模拟现实生活，每个“对象”都对应有其特定的方法，并被封装(包含)，只能通过特定的消息(即输入)访问（类=>对象）。从安全的角度来看，面向对象的编程提供了一个抽象的黑盒子。用户需要知道一个对象的接口的细节(对应于每个对象的方法的通常输入，输出和动作)，但不一定需要知道对象内部如何有效地使用它来工作。对象也可以表现出的替换属性，它允许不同的对象提供兼容的操作，以取代彼此。OOP 的优点是：模块化、延迟承诺（对象的内部组件改进不需要改变系统的其它部分）、可重用性、自然性。下面是一些常见的面向对象的编程术语：

•消息 Message：一条消息与一个对象的通信，或者是一个对象的输入。

•方法 Method：类中定义的操作，在一个对象中是对消息进行响应而执行操作的内部代码。

•**封装** encapsulate：为对象赋予几个属性值，将数据结构、操作功能和允许的访问方式封装到一个实体对象中，可以供其它对象或函数调用。封装实现了**数据隐藏**功能（data hiding），可以对抗静态代码审计。

•行为 Behavior：对象输出结果，行为是通过一个方法处理消息的结果

•类 Class：对一类具有共同特征的事物的抽象，类是的定义，包括行为、能够做什么以及做的方法。

•实例 Instance：包含自身方法的类的实例或者例子，实例就是对象。

•多实例化 Multiple instantiation：属于同一个类的多个对象，每个对象有不同的属性。

下面这个说法也是多实例化，是针对数据库的元组的：为同一主键创建多个不同的元组(记录)，它被不同的主体调用时，根据用户组织有不同的输出表现。

•**继承** Inheritance：子类延用父类的数据、方法和属性来生成一个类似的又有新功能的类，继承发生在方法从一个类(父类或超类)被另一个子类(孩子)继承时。

•委派 Delegation：委派是将一个对象的请求转发或者委派给另一个对象，如果一个对象没有处理消息的方法时进行委派

•**多态性** Polymorphism：多态性是一个对象的特性，当外部条件变化时它允许以不同的行为响应相同的消息或方法。即输入同一消息，会产生不同的结果。发送消息给某个对象，让该对象自行决定响应何种行为。多态性是通过：

1.接口和实现接口并覆盖接口中同一方法的几不同的类体现的。

2.父类和继承父类并覆盖父类中同一方法的几个不同子类实现的。

•**内聚** Cohesion：内聚描述了在同一个类中的方法的目的的关系强度，说明某模块可以独立执行多个少不同的任务。高内聚：可独立执行某个任务，而不影响其它模块。（就干一件事）

•**藕合** Coupling：藕合是对象之间相互作用的水平，低藕合意味着较少的相互作用。较低的藕合提供了更好的软件设计，因为对象更独立。较低的藕合是更容易解决和更新。具有低内聚的对象为了执行任务需要其他对象的大量的帮助，并且具有高藕合。（谁都别插手）

•**延迟承诺/递延承诺** deferred commitment：对象的内部组件改进不需要改变系统的其它部分。

4.失效安全和失效开放 Fail-secure and fail-open

应用程序故障时，其代码应被设计成能有效应对一般意义上的失败，有两个基本选择：

①失效安全状态：置系统于一个高安全级别(甚至完全关闭禁用它)直到管理员可以诊断问题和恢复系统正常运行。（微软的蓝屏）

②失效开放状态：允许用户绕过失败的安全控制，忽略错误的发生。

在第七域 K.2 章节也已经讲过了，受信恢复：恢复程序确保系统在发生故障或崩溃之后，能够还原到之前的状态。

系统可以被预置，使其在损坏时能够处于**故障防护状态** fail secure system 或者**应急开放状态** fail open system/fail safe system。故障防护状态的系统会在故障发生时保持在防护状态，并禁止所有访问；而应急开放状态在发生故障前保持在开放的状态，并允许所有访问。举个栗子就是，一扇自动门如果停电了，是保持关闭还是开放呢？这个取决于系统的业务运行

重要还是安全更重要。

在状态机模型中（大多数操作系统中），要实现故障防护（失效安全）。

二、数据库和数据仓库 Databases and Data Warehousing

第三域 E.3 章节就是数据库安全

1.数据库管理系统体系结构

尽管目前存在多种可用的数据库管理系统(DBMS)，最多的是关系数据库管理系统(RDBMS)，此外，也有层次式的和分布式的。

①层次型数据模型 Hierarchical data model

这是最早的数据库模型，将关联的记录和字段组合为一个逻辑树结构（就是存储了一堆离散的数据，每个数据有关于父节点和子节点的信息，这样就成了一个树，像 DNS 服务）。一个父节点有 0 到 N 个子节点，类似于组织结构图。数据是以一种树型结构组织的，树由分支(branch)或者节点(node)构成。可以认为分支就是数据记录，而分支上的叶子就是数据。层次数据库模型以一种按等级存储数据的方式，对于适合这种模型的特定应用，如生物学是非常有用的。

层次模型的一个缺点是它只能处理单树，不能在树枝或跨多层链接。

最常用的层次模型实现为轻量级目录访问协议(LDAP)模型。

②分布式数据模型 distributed data model

将数据存储在多个数据库中，逻辑上是互联的，形如整体，数据映射关系是多对多。

③关系数据库 Relational Databases

关系数据库是由行和列组成的平面二维表。行和列结构提供了一对一数据映射关系。关系型数据库的主要构件是表(也被称为关系)。每个表都包含一组相关的记录。

④网络模型 Network database Model

数据以块或记录类型来表述。块包含数据域，块与块间的行可以表述数据之间的关系。与层次模型的区别是，数据元素可以拥有多个父节点。

⑤面向对象模型 Object-Oriented Model

将面向对象编程中的对象数据模型与 DBMS 结合在一起，可存储图像、语音、视频等数据，也称为 object-oriented databases(OODBs)。面向对象的数据库使用类来定义其对象的属性和过程，比关系数据库更具有动态性，因为面向对象的数据库在需要时才创建对象，数据和过程(调用方法)在对象被请求时运行。在关系数据库中，应用程序必须使用自己的过程从数据库获得数据，然后根据自己的需求处理这些数据。

⑥对象-关系数据库 object-relational database management system ORDBMS

是一种关系数据库，也是 OODBs 的一个分支。使用面向对象语言编写软件前端，组合了关系数据库和面向对象的编程的能力，方便了代码重用和故障处理分析，并减少了整体维护工作量，更适合支持涉及多媒体、CAD、视频、图形和专家系统的复杂应用程序。数据被看作是对象，对象包括数据项的集合，以及可执行操作的集合。该模型并不需要一个高级语言（函数已经包含在对象中），用户交互更直接简单。关系模型也相应开始增加面向对象的函数和接口，从而建立一个“对象—关系”模型。

⑦数据仓库 Data warehousing

数据仓库指的是为了信息检索和数据分析，将多个异构的数据库或数据源集成为一个大的

数据库，并提供更多扩展的信息检索和分析的功能，可用于支持决策，数据挖掘，大数据运算。集成的数据一般会分类和聚类，并不做修改，就是只用不改。

数据仓库由数据集市(date mart)构成，数据集市由数据库(data base)构成。

⑧元数据 matadata

“关于数据的数据”被称作元数据(metadata)，描述了数据的结构和相互关系，通常并不存储在数据仓库 warehouse 中,而是存在具有更高保护级的数据超市/集市(data mart)中,data mart 可以被看作是建在部门一级的小型的数据仓库。

⑨终端用户数据库 End-User

就是 Dbase、Access 等文件型数据库。

2.表的结构

表就是关系。所有的数据值都是原子的（不能再细分）。

①**纵向**：列(column)、属性(attributes)、字段(field)，其数量称为度/阶次(degree)；

②**横向**：行(row)、记录(record,)、元组(tuple)，其数量称为基数/行数(cardinality)。

记录可以使用多种“键”来进行标识。键是表中字段的子集，是可以唯一标识某个记录的那个字段。搞清三种键：

①候选键 Candidate Keys。

可以用于唯一标识表中记录的属性子集。姓名、学号、身份证号什么的都是候选键。

②主键 Primary Keys。

候选键中选出的用来唯一标识表中记录的键被称为主键。每个表都要选一个唯一的最有代表性的主键。（主键不为空、主键唯一）

③外键 Foreign Keys。

外键被用于在两个表中建立关系(也称做参照完整性/引用完整性)。如果一个表包含一个“键”，它是另一个表的主键，那么这个“键”就是这个表的外键。（也就是外部链接）

关系模型有两个完整性规则：实体完整性和引用完整性，重点是主键和外键，这些规则源于 Clark 和 Wilson 完整性模型。

①实体完整性 Entity integrity 要求元组有一个唯一且非空的主键。

②引用完整性 referential integrity 要求外键在被引用表中必须存在该值主键的元组。

其实还有一个语义完整性 semantic integrity，要求符合数据结构和语言规则。在后面又把这 3 个完整性讲了一遍。

如果非主键的属性是空值，这在语言上对数据库来说是个问题，但它不是完整性问题。

3.结构化查询语言 Structured Query Language (SQL)

所有关系数据库都使用一种标准语言，即结构化查询语言(SQL)，为用户存储、检索和更改数据以及管理控制 DBMS 提供了一致的接口。不同供应商的 SQL 版本略有不同，但是都支持一个核心特性集。

有几个概念：

①模式 Schemas：描述数据库的结构，包括所有用户的访问控制权限。

②表 Tables：数据的行和列。

③视图 Views：定义为用户可查看表中的部分信息。视图为每个用户动态的创建，并提供

访问控制的粒度。

有几种子语言：

①数据定义语言(DDL)，允许创建和更改数据库的结构(即模式)。用户很少用到。

②数据库操作语言(DML)，允许用户与数据交互，增、查、改、删。

③查询语言(QL)，用户可以对数据库提出查询请求，通过报表生成器(Report generator)输出数据。

④数据控制语言(DCL)，用于控制对数据的访问，提供了对 SQL 的安全管理，要重点关注。常用 DCL 命令有：提交、快照、回滚、设置事务等。

报表生成器：以用户定义的方式生成数据打印输出。

4.数据库范式化 Database Normalization（标准化、规范化）

使数据库表遵从标准、规范的形式的过程称为范式化。最常见的三种形式是

①第一范式化形式(1NF)。

②第二范式化形式(2NF)。

③第三范式化形式(3NF)。

第三是最好的。这三种形式都满足以下需求：减少表中的冗余，消除错误放置的数据，执行其他许多内部处理任务。

5. ACID 模型

数据库的事务管理是重要的一项工作，不然数据会乱套了。任何一项数据库事务都必须具有四个特征：原子性，一致性，隔离性，以及持久性。这些属性合称为 ACID 模型。也是锁控制机制要实现的目标。

①原子性 Atomicity

数据库事务必须是原子的，也就是说必须是“要么全有，要么全无”。如果事务的任何部分失败，那么整个事务都要被回滚，就像什么也没发生一样。

②一致性 Consistency

一方面是数据的更改要与规则一致：所有事务都必须符合和遵守数据库的完整性规则等所有规则(例如所有记录都具有一个唯一的主键)；某个事务执行期间可能临时产生的任何不一致的数据是不允许被其它事务或应用使用的。另一方面是不同数据库里的数据要一致。

③隔离性 Isolation

隔离性原则要求事务彼此之间独立操作。如果数据库接收到两个更改相同数据的 SQL 事务，那么在一个事务被允许更改相同数据之前，另一个事务必须完全结束。

④持久性/稳定性 Durability

数据库事务必须是持久的，也就是说一旦被提交给数据库，就会被保留下来。数据库通过使用备份机制(例如事务日志)确保持久性。

6.数据库完整性

数据库管理系统 DBMS 最关注的是完整性，其次是可用性，最后是保密性。数据要保证实现 3 种类型的完整性：

①语义完整性(Semantic integrity)：严格遵循结构化规则和语义规则，也就是数据类型、逻辑值、唯一性约束等等操作什么的都要符合规则。

②引用完整性/参考完整性(Referential integrity)：外键必须在被引用的表中存在一个相同值的主键。任何记录（外键）都不能引用一个不存在记录或空值(null value)的主键；如果一个包含有主键的记录被删除了，被引用的记录也都必须删除掉。

③实体完整性(Entity integrity)：保证了数据实例(tuples)由主键值唯一确定，元组必须有一个唯一的、非空的主键。

实现完整性可以通过以下操作：

①回滚(rollback)：终止当前事务并取消对数据库的更改，数据库恢复至先前状态。

②提交(commit)：终止当前事务处理并执行用户的修改，如果更改不成功则回滚。

③检查点/保存点(Check point/Save point)：相当于虚拟机里的快照，是系统失效或检测到错误时，用户可以返回的位置，即系统破坏前的某个点。保存点太多会降低 DB 性能，太少则增加丢失数据的风险。

④两阶段提交(two-phase commit)：一个事务需要对多个数据库进行操作时，必须确保所有数据库要么同时都改了，要么都不改，绝不出现数据库没有同步修改的情况。所以要分 2 步走：先提交修改，各数据库临时修改、临时存储结果；然后交易监视器发送“预处理”命令；最后如果各数据库都响应了命令，监视器就发送“提交”命令，让和数据库真正存储修改后的数据，否则就发送“回滚”命令。

⑤shadow 恢复是在之前版本的数据库上重新执行事务，要求使用事务日志来识别最后一次正确的事务。

⑥交易（事务）处理 Transaction processes：用户与数据库间是同时并发多个交互的。

⑦批处理 Batch processing：多处操作按顺序绑定，一次一起执行完。

7.数据库安全

数据库的威胁：（第三域的 E.3 章节详细描述了防范方法）

①聚合 aggregation

组合从不同源获取的非敏感数据生成敏感数据的能力。

②推理 inference

观察可获取的信息推测（推断）出敏感或受限信息的能力。

③旁路攻击

用户试图绕过数据训应用的前端控制访问数据。

④并发

并发相关的问题包括使用旧数据执行过程，不一致的更新，或发生死锁。

⑤死锁

当两个用户同时访问信息而且都被拒绝时就发生死锁。

⑥攻击数据库视图以非法访问

用户可能试图受限视图或修改一个已经存在的视图;在数据库接口设计中经常使用的分层模型提供了一个相同数据的多条路径，不是所有的路径都受到保护。

⑦拒绝服务

任务类型的可以阻止授权用户共聚信息的攻击或行动。

⑧不当信息修改

未授权或授权用户可能故意或无意的错误地修改信息。

⑨查询攻击

用户尝试使用查询工具来访问不能正常地通过可信前端访问的数据。

⑩服务器访问

数据库运行的服务器必须防止未授权的逻辑访问同时也要防止未授权的物理访问以防止逻辑控制被禁用。

⑾数据污染

由于输入数据错误或错误的处理导致的数据完整性破坏。

⑿数据拦截（中间人）

如果允许拨号或其它类型的远程访问，必须控制拦截会话或修改传输中的数据的威胁。

⒀检查时间 / 使用时间(TOC/TOU)（必考）

TOC/TOU 也可能发生在数据库中。一个例子是，一些类型的恶意代码或特权访问可以改变数据，在用户的查询被许可时和数据展现给用户时。

⒁未授权访问

故意可无意地将信息发布给未授权用户。例如系统的错误消息或系统提示，提供了关于服务功能特性等方面的信息。

要实现多种等级的数据库访问控制和安全防护，有很多方法：

①使用视图 Views

视图可以防止聚合攻击。在数据库中实现多级安全性的一种途径是使用数据库视图。视图可以整理来自多个表的数据、聚合单独的记录或限制用户访问数据库属性和/或记录的有限子集。在数据库中，视图被存储为 SQL 语句，而不是被存储为数据表。这样可以减少所需的数据库空间，并且允许视图违反应用于数据表的规格化规则。因为视图非常灵活，所以许多数据库管理员将视图作为一种安全工具使用，就是允许用户只与受限的视图交互，而非与作为视图基础的原始数据表交互。

②并发性 Concurrency

并发性使用“锁定”功能来允许已授权用户更改数据，同时拒绝其他用户访问查看或更改数据元素。只有更改完成并“解锁”后，才允许其他用户访问。并发性或编辑控制是一种预防性的安全机制，这种机制试图使数据库中存储的数据始终是正确的，或者至少使其完整性和可用性受到保护。

③语义完整性 Semantic integrity

语义完整性是 DBMS 的一种常见安全特性，确保用户的动作不会违反任何结构上的规则。此外，还检查所有存储的数据类型都是有效的，符合逻辑的，并且确认系统遵守任何和所有的唯一性约束。

④时间戳 Time stamp

通过标记日期和时间来维护数据的完整性和可用性。

⑤细粒度控制 granularly

DBMS 的另一个常见安全特性是在数据库内能够细粒度控制对象。例如：内容相关的访问控制（基于内容）Content-dependent，分析内容之间的关系来阻止用户访问与他无关的数据，

或者有利益冲突的数据。

⑥单元抑制 cell suppression

对单独的数据库字段或单元隐藏或强加更安全的约束。

⑦上下文相关的访问控制（基于上下文环境）Context-dependent

上下文相关的访问控制通过宏观评估来制定访问控制策略，它分析每个对象、数据包或字段如何与总体的活动或通信相联系，在较大的上下文环境中就会表露出是有益的还是有害的。

⑧数据库分区 database partitioning

数据库分区技术可以防止聚合和推理漏洞。

⑨多实例 Polyinstantiation

在同一个关系数据库表中两行或更多行具有相同的主键，且为不同密级的用户提供不同的数据查询结果，就是多实例。主要防范推理攻击。（这个点经常考到）

⑩噪声和干扰 false or misleading data

在 DBMS 中插入错误的或伪造的数据，从而重定向或阻挠窃密攻击。但一定要确保插入到数据库中的噪声不影响业务运营。

⑪锁控制

锁用来控制读和写访问特定的关系系统中的数据行或面向对象系统中的对象。可以在表，行，记录，或甚至字段上加锁，这些相关的要求也被称为 ACID 测试。

8.数据库接口

考各种接口语言的特点和安全问题。

①开放数据库互连(ODBC)

访问数据库的用户名和密码以明文存储。

微软的数据库连接 API，开放数据库互连(ODBC)是一种数据库特性，不必对互联互通的数据库直接进行编程，允许应用程序与不同数据库类型通信。也就是应用程序和后端数据库驱动程序之间的代理。ODBC 还有一种 API 接口的集合，即 ActiveX 数据对象(ADO, ActiveX Data Objects)。

②JAVA 数据库连接（JDBC）

JDBC 是 Sun 公司开发的 API，用于 Java 程序连接数据库。它可以使 Java 程序直接或通过 ODBC 连接到数据库。要考虑清楚用户的鉴别和访问控制。

③可扩展标记语言（XML）

安全性最低。XML 本身是明文的。

XML 是一种标记语言，可用中性的格式来表示数据，独立于数据库和应用，以及底层的 DBMS。无线标记语言（WML）是一个基于 XML 语言的实例，它把用于蜂窝电话，寻呼机和个人数字助理(PDA)之类的通信。

④对象链接和嵌入数据库（OLE DB）

替代 ODBC 的。对象链接和嵌入(OLE)是 Microsoft 的一个技术，允许一个对象，例如 Excel 电子表格，嵌入或链接到另一对象内部，例如 Word 文档。OLE 使用组件对象模型(COM)协议。对于对象嵌入，一个提供数据或图像的应用(源)将被包含在另一个应用(目标)的文档中。目标应用并不了解或有能力编辑它，只是简单地显示或打印。要想编辑或更新嵌入的对象，它必须

在创建它的应用中打开。这一般双击会自动打开编辑。

OLE DB 是一个底层接口，由 Microsoft 设计用来跨不同的 DBMS 链接数据。它是一个开放的规范，它的设计基于 ODBC 的成功，提供了一个访问所有类型数据的开放标准，它在客户端或服务器上可作为中间件运行，可跨越很多不同的应用。它使组织可以轻松地利用信息的优点，这些数据不只存在于 DBMS 中，也包括当从其它类型的数据源访问数据时。(但仅限于 Windows 接口应用)。OLE DB 架构提供组件，例如直接数据访问接口，查询引擎，游标引擎，优化器，业务规则和事务管理。

当开发数据库和决定数据如何跨应用链接，或者通过 ODBC 接口或者通过 OLE DB 接口，则必须在开发阶段考虑安全。

⑤ActiveX 数据对象（ADO）

新的浏览器实现了沙盒和强 ActiveX 控制以帮助防范此漏洞。

ADO 是 Microsoft 针对所有类型数据的高层接口。它可以用来创建一个前端数据库客户端或中间层业务对象，其使用一个应用，工具，或 Internet 浏览器。开发人员通过使用 ADO 可以简化 OLE DB 的开发。对象可以是 Java，JavaScript，VB 和其它面向对象语言的构建组件。通过使用公共和可重用的数据访问组件(组件对象模型(COM))，不同的应用可以访问所有数据而不管数据的位置或数据格式。ADO 可以支持典型的客户/服务器应用，HTML 表格，电子表格和电子邮件引擎信息。注意很多安全专家都担心 ActiveX 的使用，因为无法配置它访问底层系统的限制。新的浏览器实现了沙箱和强 ActiveX 控件以帮助减轻此漏洞。

9.通过 Internet 访问数据库

互联网访问的通用方法是创建一个分层的架构，分层管理数据，最典型的是三层方法：

①表示层；②业务逻辑层；③数据层。在 B.5 章节 API 安全内容里也讲到了。

10.元数据

关于数据的信息，被称为元数据(关于数据的字面数据或关于数据的知识)。它提供了一个系统的方法来描述资源和改进信息的提取。目标是帮助用户通过各种源及更好的精度搜索。它包括与一个应用系统或一个信息、对象关联的数据，目标是描述，关联，法律要求，技术功能，使用，和保存。它被认为是开发和使用数据仓库的关键组件。元数据有用是因为它提供了：

①数据之间的无法发现的关系；

②关联之前被认为没有关系的数据的能力；

③打开数据仓库内的重要或非常重要数据的钥匙；

唯一考点：元数据是数据中的数据。

11.联机分析处理/在线分析流程(OLAP)

OLAP 最大的安全问题是；并发和原子。

包含在数据仓库中的数据通常都是通过前端分析工具访问，例如联机分析处理（OLAP）、数据挖掘，或数据库知识发现（KDD）方法。OLAP 技术使一个分析师能定制查询，并且基于查询的结果，定义进一步的查询。分析师可以通过在数据间漫游来收集信息。收集到的信息展现给管理层。因为数据分析师要解释数据的含义，他或她应具备关于组织的深入了解和组织需要什么类型的知识以适当的获取信息，用于决策支持。

①联机事务处理 OLTP(On-Line Transaction Processing)

用于数据库集群 DB cluster，提供容错和高性能。可以监视问题并正确处理问题，确保要么都正确，要么都不改。

例如，如果一个进程停止运作，那么 OLTP 内的监控机制能够检测到这个问题并试图重新启动该进程。如果这个进程不能重新启动，那么对应的事务处理将会回滚，从而确保事务处理的完整性或者数据不出现说误。任何检测到的错误或无效事务处理将会记录到事务处理日志中。事务处理日志还收集成功事务处理的活动。在执行事务处理前后，数据都将写入日志，以便建立一个事件记录。OLTP 的主要目标是确保事务处理的正确发生或根本不发生。通常，事务处理表示一些不可分割的操作独立发生。如果其中一个操作失败，那么其余操作需要回滚，以确保只向数据库输入准确的数据。

②数据挖掘 data mining

用于揭示隐藏关系。数据挖掘也称为数据库知识发现 **KDD**(Knowledge Discovery in Database)。除了 OLAP，数据挖掘是另外一个过程(或工具)，其通过对数据执行查询来发现数据仓库中的信息。数据挖掘是一个决策支持技术，基于一系列的分析技术，其借鉴于数学，统计学，和遗传学。该技术独立地且与其它技术协作从数据仓库中发现信息。数据发掘用于揭示隐藏的关系，模型，和数据仓库中的趋势，其是要进行数据挖掘的大量数据的知识库。

数据挖掘既可以发现潜在的入侵，方便审计；也可以用来推理攻击，发现有用的情报。

KDD 用于发现潜在模式或知识的最常用的 3 种方法：

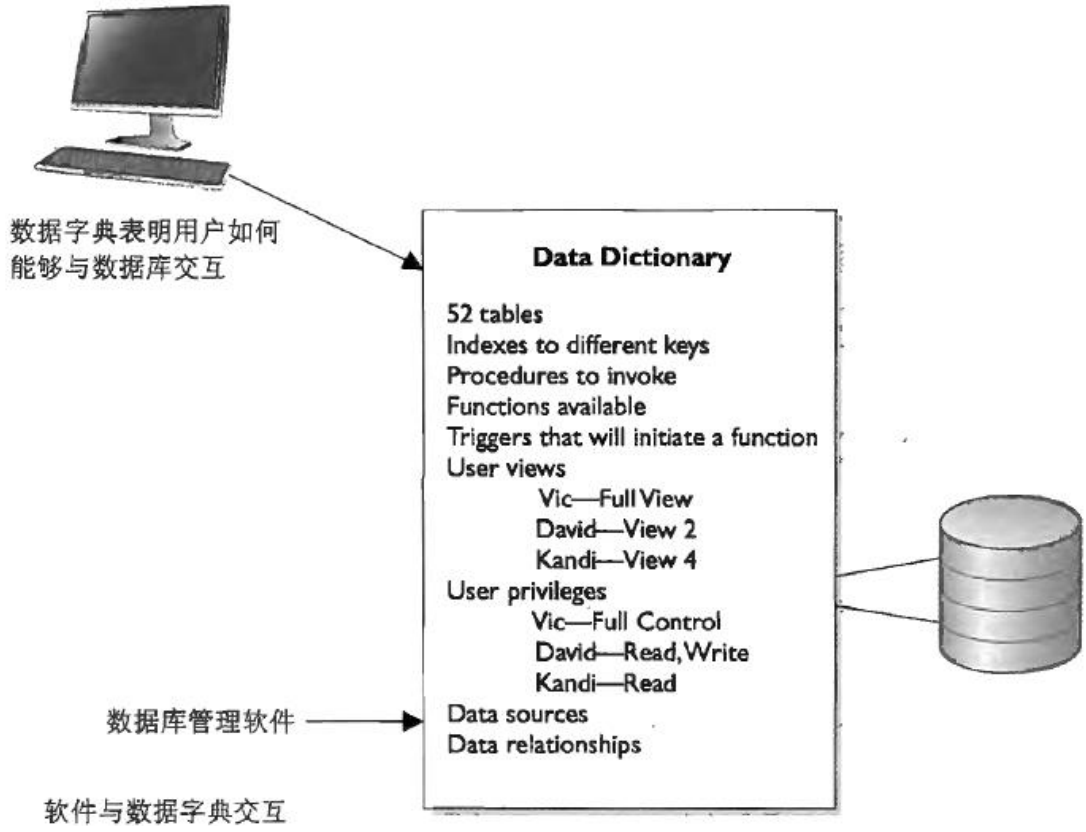
①分类 Classification。根据共同的相似性对数据分组。

②可能性 Probability。标识数据之间的相互依赖关系，并将可能性应用于它们的关系。

③统计 Statistical。标识数据元素之间的关系，并使用规则发现。

10.数据字典(Data Dictionary)

数据字典是描述数据元素及其关系的基础库，存储了数据用法、关系、来源和格式等关键信息，是数据元素定义、架构对象(schema object)和引用键(reference key)的集合，用来对数据库的数据结构进行集中管理控制。数据库管理软件读取数据字典，确认架构对象存在，并检查特定用户的进程访问权限。在数据字典中还定义了对每个用户的视图权限设置，如果要改变数据库的架构，如增加表、字段、记录、视图什么的，必须先更新数据字典。



三、基于知识的软件系统 KBS

有 3 种类型的以知识为基础的人工智能系统，用来用入侵检测分析是很准确的。

1.专家系统 Expert Systems

专家系统是不可能模拟出人类的情绪的，只能干下象棋的事，一般用于某个专业领域，通常被 IDS 用于自动检查安全日志。有两个主要的组件：知识库和推理机。

①知识库，包含专家系统已知的事实和规则 rules（就是对各种情况的判断 if/then）。

②推理机/推理引擎 inference engine，利用逻辑推理和模糊逻辑技术将输入的信息与知识库进行对比分析，并基于过去的经验做出结论。

基于规则的编程(rule-based programming)是开发专家系统的通用方法。规则基于 if-then 逻辑单元，规定了一组用于在特定情况下执行的动作。这是用专家系统寻找模式的一种方法，称为模式匹配(pattern matching) 。

模糊逻辑 Fuzzy Logic

通过使用模糊的界限，允许算法思考控制人类思维的“灰度梯度”。专家系统通过下列 4 个步骤或阶段来使用模糊逻辑：模糊化 fuzzifi cation、推理 inference、合成 composition 以及逆模糊化 defuzzifi cation。

2.人工神经网络 Artificial Neural Networks

人的大脑用模式 pattern 来存储信息，用神经元 neuron 来记忆和思考。在神经网络中，计算单元链被用来模仿人脑的生物学推理过程，用计算单元来模仿神经元。即建立 1 个计算机单元分析判断输出、互相关联、最终生成相关结果的计算决策长链。神经网络的优点包括线型、输入-输出映射和自适应性。在用于语音识别、脸部识别、天气预报和意识与思考模型研究的

神经网络实现中，这些优点十分明显。具体的算法就搞不清楚了。

神经网络可以自学习，这种活动被称为 Delta 规则或学习规则。

3.决策支持系统 Decision Support Systems

决策支持系统(DSS)是一种知识型应用，它分析业务数据并且以更容易作出业务决策的形式提供给用户，一般以图形方式提供信息，并有某个数据库的专家系统的支持。

A.1 开发方法论（例如：敏捷开发、瀑布模型）

在系统生命周期中使用的术语五花八门，不同书写的都不一样，这没关系，CISSP 考的是你对基本原理的理解。

1.包括安全管理的标准的软件开发流程

在 officail guide 7 里是这么写的 7 个阶段：

①概念定义 Conceptual definition。发布包含项目目标和系统需求的声明。（立项报告）

②确定功能需求 Functional requirements determination。完成需求规格说明书。

③控制规范开发 Control specifications development。研究提出实现所有安全功能的系统开发的方法规范。

④设计评审 Design review。上面的②是功能规格，③是控制规格，之后就是写代码做开发。等设计团队搞完了，就要开评审会议了，确保开发的方向正确。

⑤代码走查 Code review walk-through。编码设计的各个阶段都要安排几次代码走查，这些技术会议只组织开发人员，对特定的代码进行走查，寻找逻辑错误或其他设计/安全缺陷。

⑥用户验收测试 System test review。交房、验房、收房。

⑦维护和变更管理 Maintenance and change management。系统已经部署使用了。

重点了解下面这个流程：

在 CBK 里是这么写的，一般包括 7 个基本阶段和 2 个附加阶段：

①项目启动与规划 initiation。（系统建设与安全建设要同步规划、同步实施）

②功能需求定义 functional requirement definition。

③系统设计规范/规格说明（建模）system design specification。

④开发与实施 development and implementation。

⑤文档管理与版本控制 documentation and common program controls。

⑥测试和评估控制（认证与认可/认证与确证）testing and evaluation controls(certification and accreditation/Verification and Validaion)。（不能用生产数据，会泄密的）

⑦交付使用（部署上线）transition to production(implementatoin)。（开发、测试、生产环境要互相物理隔离）

附加阶段，是系统生命周期（SLC）多出来的 2 个阶段，不是系统开发生命周期 SDLC：

⑧运行与维护支持（安装后）operation and maintenance。

⑨修订和系统升级 revisions and system replacement。

软件需求可以用 3 种模型来表示：

①信息模型。规定要处理的信息类型和处理方式。

②功能模型。概述应用程序需要执行的任务和功能。

③行为模型。解释在具体事务处理发生过程中和发生之后应用程序的状态。

2.软件开发生命周期(SDLC)模型 software development life cycle

SDLC 用来规范软件开发实践。很多模型是交叉的。模型是什么大类不重要，重要的是掌握各种模型的优、缺点。

1.瀑布模型 Waterfall Model

按标准流程一步一步走，不能改顺序；上一步骤全部完成，才能进入下一个步骤；一个步骤出问题，就回到上一步骤来纠正（即反馈回路特性 feedback loop characteristic）。

①螺旋模型 Spiral Model

一个瀑布式过程的多次迭代，也可以封装许多其他模型，他被称为一个元模型，即“模型的模型”，就是走完一个模型流程，再走一遍，每次有所改进就行了。它的特点是在时间轴上的每一个阶段内，运用戴明环模型（PDCA）（计划-执行-检查-行动），突出**风险评估**，基于风险评估对成本、计划等进行调整，并决定项目是继续还是取消。在每一个阶段内，也有运用其它四个阶段的流程：制定计划、风险分析、开发和测试、客户评估。模型中的角度代表进步，螺旋半径代表成本。

②净室模型

也是瀑布的一种，可用于控制软件缺陷，目标是初写的代码必须要完善无错，不在事后找 BUG。从安全角度看，前期充分考虑安全防护比后期附加保护的效果要好。

③V 型模型（总-分-总的瀑布）

V 型模型在瀑布模型之后出现，取代软件开发过程中扁平的线性方法，它与瀑布模型一样按照顺序路径开发，每个阶段必须完成之后下个阶段才能开始，但成功概率更高。因为先从上到下的细化设计，再从下到上的单元集成，每个阶段都要通过测试才行。

2.迭代开发/增量模型

纯瀑布模型是高度结构化的，不允许返回前一阶段再作更改。而迭代方法是不断改进完善的，需要一个变更控制机制。

①原型：先构建一个简单的初始软件版本。

*快速原型/敏捷开发（RAD）：原型的一种特殊实现，在每个阶段有严格的时间限制，如果决策变化太快，软件质量可能不够高。（这种原型用于演示，用完就丢，不作最终产品）

*改进的原型模型/演化原型（MPM）：原型的一种，用于 Web 应用开发，渐进式改进，非常灵活。（实验室里开发的原型，测试后，将成为最终产品）

*运行原型：是演化原型方法的延伸，是已经安装部署在实际运行环境中的原型，微调后即可继续使用在生产环境中，其软件变更都发生在工作场所。

②联合分析开发（JAD）：最初用于开发大型机系统，逐步演进为 RAD 模型、Web 开发模型或其它模式的组成部分。它是一个管理过程，联合用户与开发人员协同工作，加强沟通，提高功能的满足度。但大量的参与人员可能影响系统在安全设计方面的考虑。

③探索模型：综合考虑所有可能的需求来建立一个有前瞻性的系统，由于缺少结构化，安

全需求可能处于次要地位，一般有特殊要求时才考虑。

④敏捷软件开发 Agile Software Development

是一种以人为核心、迭代、循序渐过的开发方法，快速的灵活的开发方法，有很多变种模型，是几个开发方法的总称。如：Scrum（迭代式增量软件开发过程），敏捷统一过程(AUP)，动态系统开发模型(DSDM)，和极限编程(XP)。它有 4 大特点：

1)实践检验，working software is the primary measure of progress;

2)简单高效，simplicity is essential;

3)绑定需求，business people and developers must work together daily;

4)当面沟通，the most efficient method of conveying information is face-toface。

⑤增量模型：类似于“多个瀑布”周期出现在同一个软件上，在开发阶段不断走向成熟。使用增量模型时，每一个增量阶段都会产生一个可以交付、 可运行的产品。

3.其它方法和模型

也有软件开发方法不依赖迭代或不分块迭代，如：

①计算机辅助软件工程（CASE）：使用辅助工具软件来进行系统的分析、设计、开发、实施和维护等，常用于大型系统开发。它为规划师、设计师、编码人员、测试人员等提供了个共享资源、协同工作的机制。

②基于组件的开发：将功能拆分为组件进行编码并按标准进行封装，而不是单独开发某个业务功能，可以节约成本、加快进度。从安全的角度看，当组件进行过安全测试后，可以被重复使用。这与面向对象的编程（OOP）类似，设计对象和类时就要考虑安全因素，并实例化。

③重用模型：基于现有的组件来构建应用，该方法最适合用于面向对象开发的项目，因为对象可以被导出、重用或者修改，并可基于已知的安全特性进行选择。

④极限编程（考点）：一种基于沟通和反馈的简单化的软件开发方法，它是一种相当结构化的开发方法，依赖于子系统的功能限定、范围定义和结对编程。团队通过发布一系列小且集成安全的软件来满足用户需求。

⑤有三种原型法，上面也讲过了：

快速原型法(rapid prototype /throwaway)：开发团队尽可能迅速的“粗制滥造”的开发出原型用于测试，在掌握精细需求和确定高效方法后，这个原型一般就丢弃了。

进化式原型法(evolutionary prototype)：不断改进目标的方式进行开发，原型会持续改进直到产品最后阶段。

操作原型(operational prototype)：是进化式原型的升级，也不断完善，但不是等交付一个版本后来改进，而是边用编写，在生产中不断调整。

A.2 成熟度模型

1.软件能力成熟度模型 Software Capability Maturity Model

软件工程研究所(SEI)在卡内基梅隆大学介绍了软件能力成熟度模型，也被称为软件能力成熟度模型(简称 SW-CMM，CMM 或者 SCMM），它的目的是帮助软件组织提高其软件过程的成熟度和质量，从一个临时的、混乱的过程，通过一个渐进的路径实现成熟的、严格的软件过程。因为软件质量取决于其开发过程的质量。此外，国际标准化组织（ISO）在其 ISO-9000 技术标

准族中对软件开发进行了规范，即 ISO/IEC 90003：2004，该标准为企业使用 ISO-9001：2000 时提供指南，其内容包括软件及相关服务的采购、供应、开发、操作和维护。

目前业内有几种不同的 CMM，容易使人混淆。CMMI 开发汇总了众多不同的成熟度模型，使其可以用于一个框架之中,已经取代了 CMM。能力成熟度模型集成 CMMI(Capability Maturity Model Integration)，集成了一整套产品和软件开发指南。它涉及软件开发生命周期的不同阶段，包括概念定义、需求分析、设计、开发、集成、安装、操作、维护等阶段，以及每个阶段应该做什么。可以根据该模型来评估安全工程实践并标识改进方法。客户也可以根据它来评估软件供应商，最理想的情况是二者结合，即软件供应商使用该模型提升流程，而客户使用该模型评估供应商的能力。

SW-CMM 的成熟度级别如下：IRDMO-初、重、定、管、优

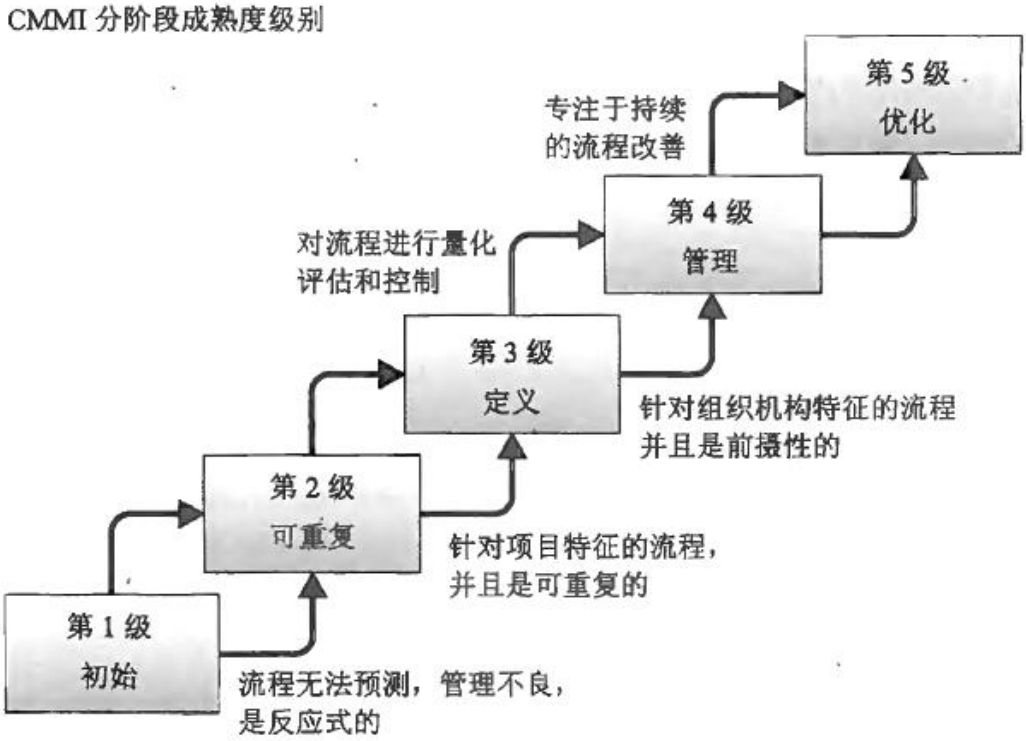
***第一级：初始级 Initial。**小作坊杂乱作业，没有定义软件开发过程。

***第二级：可重复级 Repeatable。**有基本的项目管理制度，控制费用和时间，管理人员可及时发现问题，采取措施。

***第三级：已定义级 Defined。**有一套正式的、文档化的软件开发过程进行运作。所有开发项目都在标准管理模型的约束下进行。SEI 定义这个级别的关键过程有：组织过程定义、组织过程焦点、培训大纲、软件集成管理、软件产品工程、组织协调、专家评审等。

***第四级：已管理级 Managed。**利用定量措施，以获得对开发过程的详细掌握和管控，包括：定量过程管理和软件质量管理。

***第五级：优化级 Optimizing。**开发过程不仅量化可控，还不断改进完善。



新的专门针对安全软件开发成熟度的模型有：

①SAMM，Software Assurance Maturity Model

②BSIMM：在成熟模型中构建安全 Building Security In Maturity Model

2.IDEAL 模型

软件工程研究中心也为软件工程开发了 IDEAL 模型，它实现了许多 SW-CMM 的属性，可以用来做变更管理。它将开发模型和过程划分为五个阶段：

①I：**启动阶段** Initiating。掌握业务需求，构建基础架构，筹备开发工作。

②D：**诊断阶段** Diagnosing。分析组织当前的状况，并提出应对变化的建议。

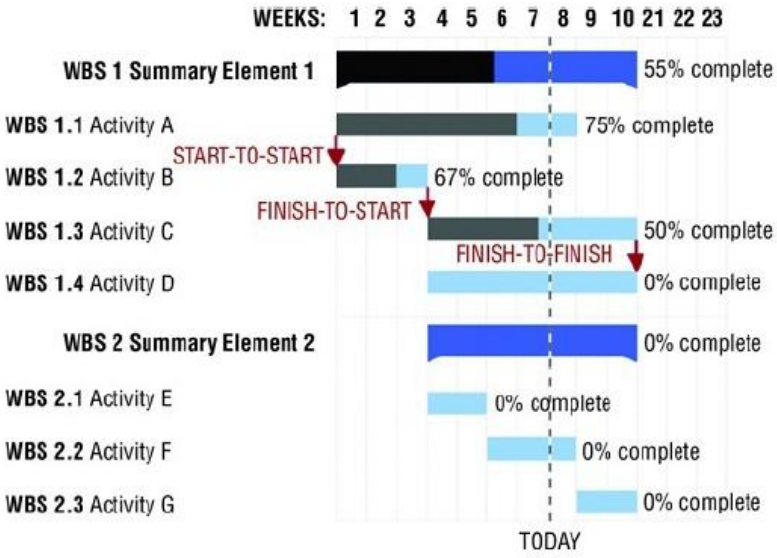
③E：**建立阶段** Establishing。采取上面的建议，计划并实施具体工作来应对变化。

④A：**行动阶段** Acting。根据详细解决方案实施具体内容，如测试、提炼、实现等。

⑤L：**学习阶段** Learning。持续分析它的效果，改进完善相关行动。

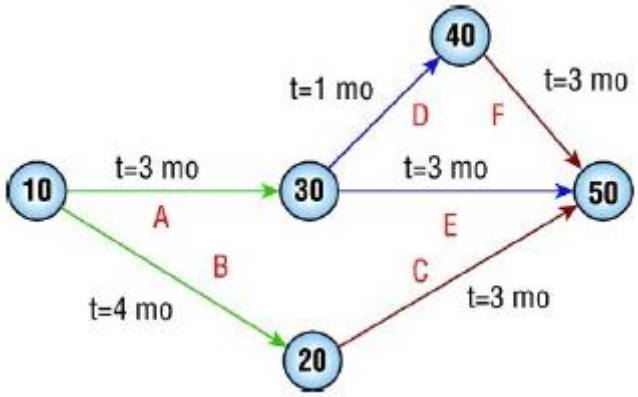
3.甘特图 Gantt Charts

甘特图是一种以条状图的方式表示特定项目和计划之间的时间关系。提供了一个图形化的图标说明，有助于在项目中计划、协调和跟踪特定任务。就是纵向任务线、横向时间轴的项目计划示意图。



4.计划评审技术(PERT) Program Evaluation Review Technique

(PERT)是一个项目调度工具，用来判断在开发软件产品和计算标准差(SD)时的风险评估方法。PERT 近似的估算出三个时间值，即最短、最长和最有可能持续时间。PERT 被用来直接改善项目管理和软件编码以制造更有效的软件。由于编程和管理能力提高，软件的实际生产花费的时间应该是较小的。



A.3 操作与维护

在系统部署应用后，要监控系统性能并保证操作的连续性，包括：检测缺陷、管理和预防

故障、故障恢复以及系统变更改进等。安全性管控包括：测试备份与恢复机制、确保对数据的处理正确无误、确保安全功能有效。

在维护阶段，发生重大变更时，要周期性的进行风险分析并对敏感应用重新认证，以验证系统的安全功能未受影响，并指定专人对系统的功能和服务水平进行验证，确保系统满足使用需求和安全基线。

A.4 变更管理

1.变更管理的工具软件

Tripwire，用来监测数据完整性的工具，可以辅助监控系统的变化。也可以将 Tripwire 的通知和告警信息集成到监控中心进行关联分析。

2.变更管理流程的三个基本组件：

变更控制（change control）是管理所有产品或系统变更的系统化方法。目的是确保不实施没必要的变更、所有的变更都得到证明、服务不受不必要的干扰且资源都有效利用。在 IT 领域中，变更控制是变更管理（change management）的一部分。

①请求控制。Request Control provides a framework for user requests.

②变更控制。Change Control。控制变更使其符合质量要求，正确记录编码的任何变化等。

③发布控制。Release Control manages the deployment of code into production.在发布新的软件之前，要进行双重检查，确保调试代码或后门都被清除，还要控制软件版本。

如果有变更实施了，影响了其它系统，就要实施配置管理 Configuration control 了，它有四个主要组成部分：配置识别、配置控制、配置状态报告、配置审核。Configuration control ensures that changes to software versions are made in accordance with the change and configuration management policies.

3.变更管理的关键点是：

①必须有严格规范的过程管理，确保质量。

②必须按规定进行请示报批、测试和记录。

③必须有应急恢复措施以防变更失败。

4.变更的流程

①请求变更 Request。

②影响分析/影响评估 Impact Assessment

③审查变更 Review

④批准/不批准 Approve/reject/Approval/Disapproval

⑤构建和测试 Build and Test

⑥通知/通告 Notification

⑦实施变更 Schedule and implement。

⑧验证 Validation

⑨记录/版本更新和基线 Document。

A.5 综合性产品团队（例如： 开发运营）

也有翻译成“集成产品团队”的，也就是 XX 课题攻关小组。Integrated product team。

集成产品和过程开发（IPPD）Integrated Product and Process Development，是一种管理技术，通过 1 个综合性的团队来优化设计、生产和服务的过程，包括必须的采购活动。IPPD 的一个关键原则是：通过综合性产品团队（IPTs）来实现多学科团队协同工作。（中国的单位经常为了应对某一任务临时抽组各部门的人员成立的专项工作小组）

1.DevOps 方法

DevOps 是用于提高软件开发效率的一种**项目管理方法及过程**（一个模型）。软件工程一般存在软件开发、质量保证和技术操作（Software development、Quality assurance、IT operations）这些重要职能之间严重脱节的情况，不同团队的个人，各司其职，往往相互矛盾，导致了在创建代码、测试和部署到生产环境之中的环节产生冗长的时间延迟。当问题出现的时候，他们不是一起合作解决问题，团队之间常常将问题抛给对方，导致反复地官僚主义。DevOps 方法旨在通过将三种职能融合在在一个单一的运作模式下来解决这些问题。DevOps 这个词是开发 Development 和运行 Operations 的组合体，标着着这些功能必须合并和合作去满足业务需求。DevOps 模型与敏捷开发方法关系紧密，目的都是为了减少开发所需的时间、以及测试和部署软件的变更。使用 DevOps 模型可以很轻松的在 1 天时间内多次部署代码。

①支撑 DevOps 构件的核心公共原则（考点）：

*对原型系统进行开发和测试。

*使用可重复的、可靠的流程进行部署，促使开发和运营以迭代的方式稳步发展。

*实时智能地监控和验证运营质量。

*形成闭环管理：企业建立对接机制，让所有利益主体掌握并及时有效处置各种反馈。也称为放大反馈环，这项原则呼吁组织建立沟通渠道，让所有利益相关者访问并对反馈采取行动。

②目标：

流程的自动化。

③最终目的：

提高客户响应能力。

B. 在开发环境中执行安全控制

B.1 软件环境的安全

软件开发在需求阶段进行安全策略设计是最节约成本的。（越早做安全越好）

1.Web 安全

由于 web 系统和应用的可访问性，输入验证是关键，应用代理防火墙在这方面最适合，但要确保代理可以处理缓冲区溢出问题，身份认证问题，编码问题(例如 Unicode)，和 URL 编码和转换等。

①开放 Web 应用安全项目(OWASP)/如何确保网站安全（必考）

在第八域 B.1 章节也讲了。OWASP 是一个致力于提高软件安全性的非营利机构。OWASP 开发了大量免费的实用产品，其中包括：

①OWASP 十大项目：基于 Web 应用存在的十大缺陷给出抑制它们的方法。

②OWASP 指南项目：一部说明如何设计出安全的 Web 应用和服务的全面手册。

③OWASP 软件保障成熟度模型(SAMM)：SAMM 是一个框架，用于针对机构面临的具体风险量体裁衣地设计软件。

④OWASP 移动项目：为开发人员和架构师开发和维护安全移动应用提供了资源。

有鉴于基于 Web 和基于云的解决方案使用得非常普遍，OWASP 提供了一个带 Web 应用安全流程的可访问全面框架。你应该对 OWASP 的作品有一个全面的了解，搞清如何将其应用到自己的任务中。OWASP 识别出的 10 大顶级风险有：

A1：注入；A2：跨站脚本攻击(XSS)；A3：无效的认证和会话管理；

A4：不安全的直接对象引用；A5：跨站请求伪造(CSRF)；

A6：安全配置错误；A7：不安全的加密存储；A8：URL 访问限制失败；

A9：薄弱的传输层保护；A10：未经验证的重定向和转发。

②Web 应用安全联盟(WASC)

Web 应用安全联盟(WASC)是一个组织，它为 World Wide Web 和组成万维网的基于 Web 的软件提供了最佳安全实践标准。这个组织提供了一系列的资源、工具和信息，可以通过它们了解这些基于 Web 的软件开发中常见的安全问题以及如何避免它们。该组织拥有一个 Web 应用程序扫描评估标准，可用于评估各种厂家的产品和实践。它提供了 Web 应用程序的安全指标和威胁分类，并维护着蜜罐进行实时超文本传输协议(HTTP)的 Web 威胁流量分析。这个组织阐述的最常见的顶级攻击方法有：

①跨站请求伪造（CSRF）；②跨站攻击（XSS）；③拒绝服务攻击（DOS）；

④已知漏洞；⑤暴力攻击；⑥隐藏参数操作；⑦网银木马；⑧点击劫持。

③关于输入验证的攻击

客户端都要通过发送指令、表单什么的请求 WEB 服务，必须要对 WEB 输入的内容进行验证，不然会因为输入一些特殊字符而被攻击。如：

1.路径/目录遍历(Path or directory traversal)：这个攻击又被称为“点-点-斜线”、“../”dot dot slash；在 URL 中接入几个“../”就可以访问上级的文件目录了。

2.统一代码编码(Unicode encoding)：Unicode 是一种行业标准，开发他的目的是为了以标准的编码格式来表示世界上的 10 万多个文本字符。Web 服务器通过 Unicode 来支持不同的字符，在 Unicode 下，攻击者不用“../”来攻击，而使用 Unicode 的“%C1%1c,%c0%9v,and %C0%af”来攻击。

3.网址编码(URL encoding)：在 URL 中，“空格“表示为“%20”，其实其它字符也可以在 URL 里用特殊的方式来发送。

4.客户端验证(Client-side validation)：是指将指令发送到服务器之前在客户端进行验证，如果黑客劫持攻击者环境，插入恶意数据，也就绕过了这个验证了。

还有缓冲区溢出(buffer overflow)、SQL 注入、XSS 什么的，后面的应用程序安全里讲，这里不解释了。

2.开源

开源的不好就是，它的漏洞问题可以更广泛、更容易的被其它人发现。

开源的开放性能促进快速的识别和修复任何问题，包括那些与安全相关的问题。有一种安全称为“隐晦安全”的想法，即如果一个系统不为人知，它被人找到如何攻破的可能性就会降低。也就是越小众的系统，暴露的漏洞也越少。

全面披露：指发现安全漏洞的个人应公开的传播此信息。

3. Java 安全

在字节码被解释的时候，Java 检查应用使用的变量和内存。这种检查对于安全可能是好事，或坏事。通常，这是件好事，因为程序正确的使用内存且不超出设定的边界。但是，过分依赖这些功能，如果开发者不在他们的代码中使用额外的安全检查，可能引起马虎的作风以致引起其它安全问题。例如，Java 通常被认为非常善于垃圾收集，自动的内存单元的检查，和不再需要的内存的取消分配。这是好事，它确保程序不会充满所有可用内存然后运行遇到问题。但是，这个语言没有办法决定信息的敏感性，它可能存储于那些内存单元。因此，它可能导致敏感信息被不正当的泄露。不提供垃圾收集服务的语言要求程序员关于内存分配做出自觉的选择，并且这种选择可能提示程序员在其返回可用内存池之前，覆盖内存单元。

Java 安全方法的三个部分(有时被称为层)是（考点）：

①验证器(或翻译器)interpreter：有助于确保类型安全；它主要负责内存和边界检查

②类加载器：从 Java 运行时环境动态地加载和卸载类

③安全管理器：作为安全的看护者防止恶意功能

沙箱（Sanddox）：

Java 最初是为一个分布式应用环境设计，因此安全模型建立了一个沙箱，其对分布式 Java 程序可以做什么和不可以做什么进行严格控制。一个不同于沙箱方法处理动态代码的方法是只允许可信代码运行。例如，ActiveX 控件只有在你完全信任控件签名的实体时，才可以执行。不幸的是，ActiveX 系统的设计和实现都有问题。ActiveX 没有沙箱来限制一个 ActiveX 控件的活动，它可以对可用的可执行程序执行任何行动或功能，不存在对程序的可靠性或边界限制的运行时检查。

针对是沙箱的攻击是：延时木马（在沙箱完成检验后，沙箱重置后运行）。

4. 分布式面向对象系统

（没内容可考）

很多通过使用基于分布式对象的软件系统构建，例如公共对象请求代理体系架构(CORBA)，Java 远程方法调用(JRMI)，企业 JavaBean（EJB)，和分布式组件对象模型(DCOM)。分布式面向对象系统允许系统的组件位于网络内分开的很多多计算机上。

对象如何相互通讯是复杂的，尤其是因为对象可能不是驻留在同一台机器上，而是可能位于跨网络的机器上。为了使这个过程标准化，对象管理组织(OMG)创建了一套标准来发现对象，初始化对象，和给对象发送请求。这个标准就是对象请求代理（ORB)，它是公共对象请求代理体系架构(CORBA)的一部分。

①公共对象请求代理体系架构(CORBA)

公共对象请求代理体系架构(CORBA)是一套由对象管理组织 OMG(Object Management Group)定义的工业标准，它解决硬件和软件产品之间的互操作需求。包括 2 部分：

面向系统组件(对象请求代理 ORB+对象服务 OS)，system-oriented components (object

request brokers and objectservices)；

面向应用组件(应用对象 AO+通用设施 CF)，application-oriented components (application objects and common facilities)。

对象请求代理 ORB 是中间件，管理组件中的所有通信，建立了对象之间一个客户-服务器关系，使他们能在异构和分布式环境中交互，且与运行的平台无关，提高互操性。ORB 依赖于 Object Service，以提供访问控制、跟踪、重定位对象和建立对象。ORB 就是中间件。CORBA 安全服务支持四种类型的策略：**访问控制，数据保护，抗抵赖和审计**。

EJB 是 Sun Microssystem 的模型，提供了构建可扩展，分布式，多层，基于组件的应用的 API 规范。EJB 使用 Java 的 RMI 实现通信。EJB 服务器提供了事务，安全和资源共享的标准服务集合。EJB 的优点之一是允许人员组装组件来控制访问。不是通过组件开发人员硬编码策略，最终用户(即，系统管理员或安全员)可以指定安全策略。其它安全功能也提供给最终用户。EJB 的一个脆弱性是 RMI 的著名的弱点。例如，RMI 通常配置为允许用户在代码不存在的情况下自动地从服务器下载。因此，在客户可以建立安全的连接之前，依然能够下载代码或者一个恶意的攻击者可以伪装成服务器的客户并下载代码。虽然已经做了改进，增加了 RMI 的安全性，所有的现都必须对安全功能进行评审。

②分布式计算环境（Distributed Computing Environment,DCE），

DCE 由 OSF(Open Software Foundation)开发，也被称为 Open Group，是行内第一个尝试分布式计算的框架，是一个基于 RPC 通信层的管理服务。他是 C/S 框架并被多家厂商采用。DCE 提供远程过程调用（Remote Procedure Call (RPC)）服务，安全服务、目录服务、时间服务以及分布式文件支持等。DCE 是通过客户端/服务器模型标准化异质系统通信的首个尝试，它为后来的 CORBA、DCOM 和 J2EE 等分布式计算技术提供了多个基础性概念。

DCE 使用通用唯一标识符 **UUID**(Universal Unique Identifier)来唯一标识环境内的用户、资源和组件。下面的 DCOM 则使用全球唯一标识符 **GUID**(Globally Unique Identifier)。

③分布式组件对象模型(Distributed Component Object Model，DCOM)

DCOM 支持程序中的组件交互，定义了组件内的交互关系，为简单的交互处理通信提供一个体系结构，支持分布式进程通信(IPC—InterProcess Communication)，支持应用访问网络中不同位置的对象。他类似功能的组件还有：面向消息的中间件 MOM (message-oriented middleware)、开放数据库连接 ODBC (Open Database Connectivity)等。

COM/组件对象模型(Component Object Model)是由微软发的一套标准化 API、组件命名机制和通信标准，允许同一应用内的进程间或相同计算机系统内不同应用的进程之间的通信。

DCOM 已经淘汰，被.NET Ramework 取代。

④对象链接和嵌入(Object Linking and Embedding,OLE)

程序调用另一个程序的能力称为**链接**。将一段数据放入外部程序或文档的能力称为**嵌入**。

对象链接和嵌入 OLE 为在本地个人计算机上其事对象提供了一种方式，并使用 COM 作为其基础。OLE 使对象(如图形、图片和电子表格)可以嵌入文档中。OLE 还允许链接不同的对象和文档。例如，当你创建一个包含 URL 的文档时，URL 会变成带下划线的蓝色字符，指示用户可以单击 URL 转到相应的 Web 站点；这是链接能力的一个示例。如果你在文档中增加一个电子表格，那么就是嵌入的例子。如果你需要编辑这个电子表格，那么只要双击该表格，操作系统

就会打开正确的环境(可能是 Excel)让她进行编辑修改。

在万维网(World Wide Web)中应用的 OLE 技术称为 ActiveX。ActiveX 组件与其他组件一样,但是可以进行移植。ActiveX 组件可以运行在任何支持 DCOM(使用 COM 模型)或者使用 DCOM 服务进行通信的平台上。

在前面“数据库和数据仓库”里也讲过 OLE。

5.库和工具集

软件库是由预先写好的代码,类,过程,脚本,和配置数据组成。一个开发者可能手动地为程序添加一个软件库以获得更多的功能或者自动化一个过程而不用从头开始编写代码。在计算机编程中,标准库是跨编程语言实现可用的库。标准库通常包括常用算法的定义,数据结构,和输入和输出机制。常见的编程语言库有:

*C 标准库,为 C 语言提供;

*C++标准库,为 C 一语言使用;

*框架类库(FCL),为.NET 框架使用;

*Java 类库(JCL),为 Java 编程语言和 Java 平台使用;

*Ruby 标准库,为 Ruby 编程语言使用。

6.集成开发环境 IDE

集成开发环境把很多工具的功能组合到一个软件程序,供开发人员使用。集成开发环境的设计,提供带有相似的用户界面的紧密的组件,以最大限度地提高程序员的工作效率。IDE 展现为一个单独的程序,所有的开发工作都在其中完成。有时,也包括了版本控制以帮助计算机程序员管理图形用户界面(GUI)的开发。

7.运行时 Runtime

每种编程语言都有某种形式的运行时系统,就是运行环境;不管是编译语言,解释语言,或嵌入的特定领域的语言,或是通过一个 API 调用。除了支持语言构建的行为,一个运行时系统可能也执行支持服务例如类型检查,调试,或代码生成与优化。例如,Java 运行时环境(JRE)就是当你使用 Java 软件时要用的。JRE 由 Java 虚拟机(JVM),Java 平台核心类,和 Java 平台支持库组成。JRE 是 Java 软件的运行时部分,你的 web 浏览器中需要运行的只有它。运行时系统也是网关,通过它一个运行的程序可以与运行时环境交互,它包含状态值,其在程序执行时可以访问,还有活动的实体,在程序运行时可以和其交互。环境变量是很多操作系统的功能并且是运行时环境的一部分;一个运行的程序可以通过运行时系统访问它们。

从 SQL Server 2005 开始,SQL Server 提供了 Microsoft Windows 的.NET 框架公共语言运行时(CLR)组件的集成。这意味着,现在你可以使用任何.NET 框架语言,包括 Microsoft Visual Basic .NET 和 Microsoft Visual C#,编写存储过程,触发器,用户定义类型,用户定义函数,用户定义聚合,和流表值函数。

B.2 源代码层面的安全弱点与脆弱性 (例如:缓存溢出、权限升级、输入\输出验证)

一、恶意代码 Malicious Code

病毒、木马等任务威胁计算机安全的代码。还有什么间谍软件、广告软件,不说了。

有害代码的分类:

①文件感染型病毒 File-infecting Virus；②引导区病毒 Boot Sector Virus

③邮件病毒 Email Virus；④宏病毒 Micro Virus

⑤脚本病毒 Script Virus；⑥木马 Trojan Horses

⑦远程访问木马 Remote Access Trojan,RAT；⑧炸弹 Bomb；⑨蠕虫 Worm

1.病毒 Viruses

把一个程序定义为病毒的唯一要求是它可以自我复制。

病毒的 3 个特征：隐蔽性、破坏性、可传播性。

①病毒传播 Virus Propagation

借助于大意的计算机用户可通过交换磁盘、共享网络资源、发送电子邮件或其他共享数据的手段来传播。有 4 种常见的传播技术：主引导记录感染、文件感染、宏感染和文件注入。

引导区病毒，引导扇区和主引导记录 master boot record infection

主引导记录 MBR 是一个单独的磁盘扇区，通常是在启动过程的初始阶段读取的介质的第一个扇区。MBR 决定介质的哪个部分包含操作系统，并且随后指导系统读取对应部分的引导扇区，以便加载操作系统。MBR 病毒将系统重定向到被感染的引导扇区，在从合法引导扇区加载操作系统之前将病毒加载到内存中。引导扇区病毒实际上感染合法的引导扇区，并且在操作系统加载过程中被加载到内存中。主引导记录感染主引导记录病毒(MBR)是已知的最早的病毒感染形式。由于 MBR 非常小(通常只有 512 字节)，因此它不能包含实现病毒传播和破坏功能所需的所有代码。为了避开空间的限制 MBR 病毒引导系统读取并且执行在另一个地方存储的代码，从而将全部的病毒加载到内存中。

文件程序感染病毒 file infection

感染病毒的可执行文件。

宏病毒 macro infection

用宏语言编写的病毒，独立于平台，利用应用软件允许运行脚本的功能，像 Visual Basic for Applications (VBA)什么的。由于许多应用程序都允许宏程序嵌入到文档中，当打开文档时，程序会自动运行。这提供了病毒传播的不同机制。

服务注入病毒 service injection

注入到操作系统中的可信运行进程中，如 svchost.exe 、winlogoin.exe 和 explorer.exe 等。通过成功地使这些可信的进程，恶意代码能够绕过主机上安装的任意反病毒软件的检测。

2.其它病毒类型

压缩病毒

另外一种类型的病毒，把自身附着在系统的可执行程序上，利用用户的权限压缩。

隐蔽性病毒(stealth virus)

隐藏它对文件和引导记录所做的修改，这可以通过监视系统读取文件和扇区的功能并伪造结果来完成。

多态性病毒

产生自己不同的可操作副本。多态性病毒没有任何部分相同，很难直接根据病毒特征来检测它们。

分体病毒(multipart virus)

也叫多方病毒，它有几个组件，可以分布在系统上不同部分。它以多个方式感染和传播，即便被识别也很难完全清除。

自乱码病毒(sel-garbling virus)

通过打乱自身代码使之不与预定义的病毒特征相匹配，从而可以逃避防病毒软件的检测。

大脑模仿病毒(meme virus)

实际上并不是计算机病毒，而是一种在网络上不断转发的电子邮件。

蠕虫(Worm)

它们无须主机应用程序便可自我繁殖，是自我约束程序。

其它还有：混合型病毒 multipartite、邮件病毒、脚本病毒(script virus)、隧道病毒(tunneling virus)什么的。

3.病毒技术 Virus Technologies

搞清四种类型的病毒：复合病毒、隐形病毒、多态病毒和加密病毒。

①复合病毒 Multipartite Viruses

复合病毒使用多种传播技术来渗透只有单一防御手段的系统。例如，在 1993 年发现的 Marzia 病毒既是一种文件感染程序病毒，也是一种引导扇区病毒。（有多种手段传播）

②隐形病毒 Stealth Viruses

隐形病毒对操作系统进行篡改，从而欺骗反病毒软件，将自己隐藏起来。

③多态病毒 Polymorphic Viruses

在系统间传输时，多态病毒会修改自己的代码，自动产生各种变种，使得特征型反病毒软件包失效。

④加密病毒 Encrypted Viruses

类似多态病毒，每个被感染的系统呈现不同的特征。不过，加密病毒不是通过改变其代码生成这些修改过的特征，而是修改了在磁盘上的存储方式。即对存储在磁盘上其他地方的主病毒代码进行加载和解密。因为每个感染过程都使用不同的密钥，所以感染的系统会呈现出完全不同的样子。不过，病毒解密程序往往包含指定特征，因此加密病毒很容易被更新的反病毒软件包识破。

3.逻辑炸弹 Logic Bombs

逻辑炸弹是感染了系统但一直保持休眠状态的恶意代码（病毒），当达到或满足一个或多个逻辑条件(例如时间、程序启动、Web 站点登录等)时，它被触发。

4.特洛伊木马 Trojan Horses

各种木马，不解释。是恶意代码，不是病毒。

5.僵尸网络 Botnets

僵尸网络(botnet)由 Internet 上被僵尸主控者/僵尸牧人(botmaster)控制的众多计算机(肉机 bot)组成。

6.蠕虫 Worms

蠕虫是不需要任何人为的干预就可以自我传播的病毒。互联网上发生的首例安全事件就是蠕虫病毒。可以关注一下震网病毒（STUXNET），它是蠕虫，但它带来的更多研究都是关于 APT 攻击的。

7.反病毒机制 Antivirus Mechanisms

基本上就是特征检测了，需要一个极大的病毒特征库，如果查到病毒，有 3 各处理方法：

①如果可以杀毒，那么杀。

②如果不知道怎么杀，那么隔离，等管理员分析处理。

③如果文件无法隔离又很危险，直接删除。

另一种方法就是启发式的机制 heuristic-based mechanisms。这些方法通过分析软件的行为，来寻找病毒活动的迹象，如：试图提升权限级别，掩盖他们的电子痕迹什么的。几乎所有防病毒软件产品都使用“启发式检测(heuristic detection)”，这种方法会分析恶意代码的总体结构，评估编码指令和逻辑功能，并研究病毒或蠕虫内的数据类型。因此，它收集与这段代码有关的大量信息，并评估其作为恶意代码的可能性。这种方法采用一个“可疑性计数器”，该计数器的计数将随着程序发现潜在的恶意属性的增多而递增。如果计数器超过某个预先设定的限值，那么就确认该代码为危险代码，防病毒软件会立即采取行动以对系统进行保护。这使得防病毒软件能够检测出未知的恶意软件，而不是仅仅依靠病毒特征。

还有一种方法是 Tripwire 数据完整性保证软件包，用于检测发生了未授权的文件修改，它要维护一个系统所有存储文件的散列值的数据库来实现完整性检测。

二、应对措施

培训和明确的安全策略可以大大减少用户的危险。一些指南也给出了应对恶意软件的最佳实践：*不要双击附件；*当发送附件的时候，提供一个明确和具体的对附件内容的描述；*把不要盲目地使用应用最广泛的产品作为公司标准；*禁用 Windows 脚本宿主，如 ActiveX、VBScript、和 JavaScript；*不要发送 HTML 格式的电子邮件；*使用一个以上的扫描器，并扫描一切。

针对恶意代码的主要防护手段是使用反病毒过滤软件。这些软件都是基于特征库的，要重点关注 3 个方面的问题：一是客户端都要安装使用并更新反病毒软件；二是保护服务器更重要；三是有必要能网络通信流量进行过滤。对于没有更新库的新型病毒，也要采取相应的措施：

一是使用完整性检查软件(例如 Tripwire)扫描文件系统中异常的更改并定期报告。

二是应当严格地维护和实施访问控制，限制恶意代码传播和破坏能力。

此外，还有 3 种方法可以防范嵌入到活动进程的恶意代码：

①Java 的沙箱技术为 applet 提供了一个隔离的环境。

②ActiveX 控件签名技术利用数字签名确保代码来自可信源。

③通过白名单机制，在操作系统只允许已知的良好的应用程序运行，阻止未知程序。

1.防病毒软件的检测机制：

①特征型检测(Signature-based detection (also called fingerprint detection))：分析恶意代码特征并提取为分析恶意软件的指纹，时新病毒没有用。

②启发式检测(heuristic detection)：分析恶意代码的整体结构，评估编码指令和逻样功能，并研究病毒的数据类型。其中，审查与代码有关的信息称为静态分析(static analysis)，而允许一部分代码在受控的环境中运行，称为动态分析(dynamic analysis)。

③沙箱或虚拟机(virtual machine or sandbox)：允许可疑代码中的某种逻辑在这个受保护的环境中运行。使得防病毒软件可以动态的检查可疑代码，获得与该代码有关的信息。

④行为阻止器(behavior Mockers)

防病毒软件发展的下一个阶段称为行为阻止器(behavior blocker)，自动阻止以下行为：*写入启动文件或注册表中的 RUM 健；*打开、侧除或修改文件；*在电子邮件中插入脚本，并发送可执行代码；*连接到网络共享文件或资源；*修改一个可执行文件的逻辑等。

另一种分类将恶意软件或杀毒软件的机制分为 3 种：

迄今为止，有三种主要类型，首次由 Fred Cohen 在他的研究中讨论：

①已知特征码扫描。——类似基于签名的 IDS。

②活动监控。——类似基于规则的 IDS。

③变化检测。——类似基于统计的 IDS。

三、密码攻击 Password Attacks

1.密码猜测攻击 Password Guessing

凭经验，用一个好的密码字典就可以轻松猜解弱口令。

2.字典攻击 Dictionary Attacks

字典攻击很常见了，对于散值存储的密码可以用彩虹表来破。

至于社会工程学攻击，就不多说了，反正会忽悠比什么都来得快。

四、应用程序攻击

1.缓冲区溢出 Buffer Overflows

输入内存的数据太大，就会“溢出”其存储空间（编程函数先定义一个变量 var 什么的，执行时操作系统会给程序一个内存空间的），溢到隔壁的存储空间里，可能被正常执行了或影响别的进程了。利用缓冲区溢出漏洞可以在服务器上执行任意代码。

许多编程语言对变量的长度不强制实施限制，这就要求编程人员对代码进行边界检查。只要允许用户输入程序变量，编程人员就应当采取有效措施，确保满足下列各项条件：

①用户输入的值的长度不能超过任何存放它的缓冲区的大小。

②用户不能向保存输入值的变量类型输入无效的值。

③用户输入的数值不能超出程序规定的参数操作范围。

如果没有执行对上述条件的简单检查，那么就可能造成缓冲区溢出漏洞。

2.检验时间/使用时间攻击 Time of Check to Time of Use（必考）

也称为异步攻击(asychronous attack)，有的人把竞争条件（race condition）也看作是这种攻击，其实是不一样的，竞争条件是改变进程的顺序（排序）；TOC/TOU 是进入 2 个进程之间进行更改（插队）。

检验时间到使用时间(time-of-check-to-time-of-use，TOCTTOU 或 TOC/TOU)是一个时间型漏洞，当程序检查访问许可权限的时间早于资源请求的时间时，就会出现这种问题。例如，如果操作系统针对用户登录建立了一个综合的访问许可权限列表并且在整个登录会话期间查询这个列表，那么就存在 TOC/TOU 漏洞。如果系统管理员取消了某个特殊的权限，那么这个限制只有在用户下次登录时才会起作用。如果在用户登录的时候正好发生取消访问许可权限的操作，那么用户是否能够访问资源就是不确定的。用户只需保留会话打开数天之久，新的限制就永远不会被应用。

对策：系统应当使用原子操作；操作系统可以使用软件锁。

3.跨站脚本攻击(XSS) Cross-Site Scripting（必考！）

术语“跨站点脚本(Cross-Site Scripting，XSS)”指的是利用一个 Web 站点的脆弱性，在 Web 应用程序中注入恶意代码的攻击。攻击者(用客户端脚本语言，如 JavaScript)把他们的恶意代码注入到网页中。随后，不知情的用户在访问这个站点时，恶意代码就会在他们的浏览器中执行，这样可能会导致 Cookies 被盗、会话被劫持、恶意代码被执行和访问控制被绕过，或者有助于利用浏览器的错落性。XSS 攻击的关键在于将恶意代码写入 Web 站点。一般是在一个有返回结果的表单网页里，输入带<SCRIPT>标记的字段，服务器收到表单内容就会运行里面的恶意代码了。XSS 有三种类型：

①非永久/非持久性 XSS (NonpersistentXSS)，也叫反映漏洞/反射脆弱性，出现在攻击者欺骗受害者处理一个用流氓脚本来编程的 URL，从而偷取受害者敏感信息(cookie，会话 ID 等)的时候。这个攻击的原理是利用动态网站上缺少适当的输入或者输出确证。（就是返回一个有恶意代码的 URL 给用户点击）

②永久/持久性 XSS(PersistentXSS)，也叫二阶漏洞，也称为存储或者第二顺序脆弱性，通常针对的是那些让用户输入存储在数据库或其他任何地方(如论坛、留言板、意见簿等)的数据的网站。攻击者张贴一些包含恶意 JavaScript 的文本，在其他用户浏览这些帖子时，它们的浏览器会呈现这个页面并执行攻击者的 JavaScript。（就是把恶意代码存入网站）

③基于文档对象模型/DOM 型(Document Object Model based XSS)。也叫本地跨站点脚本。DOM 是标准结构布局，代表着浏览器中的 HTML 和 XML。在这样的攻击中，像表单字段和 cookie 这样的文档组件可以通过 JavaScript 被引用。攻击者利用 DOM 环境来修改最初的客户端 JavaScript。这使受害者的浏览器执行由此而导致的 JavaScript 代码。

4. SQL 注入攻击 Injection（必考！）

SQL 注入攻击比 XSS 更加危险，它同样是向 Web 应用程序输入带特殊字符的表单字段，只是它的目的不是欺骗用户，而是访问数据库。在动态网页中，经常会让用户输入附录密码、查询关键字等表单内容，然后发送给数据库进行查询或比对。如果把输入的字段加一些特殊字符，就可以让 SQL 语言执行额外的操作，从而进入数据库。比如：正解的输入密码是“123456”；要想注入就输入“123456’; XXXXX WHERE ’a’ = ’a”，那么数据库会执行 2 条正常的 SQL 语言了。

可以通过下列三种技术来防范：

①执行输入验证。与跨站脚本攻击的防御方法一样，输入验证操作能够限制用户在表单中输入的数据类型。

②限制用户特权。Web 服务器使用的数据库账户应当具有尽可能最小的权限。

③利用数据库存储过程来限制应用程序执行任意代码的能力。存储过程就是：SQL 语句已经编写并封装好了，驻留在数据库服务器，仅可由数据库管理员修改；Web 应用程序则调用各种现成的存储过程来运行，不直接通过 SQL 语句来访问数据库。

5.侦察攻击/网络侦察扫描 Reconnaissance Attacks

目的就是找 IP、端口和漏洞。搞渗透测试必须技能，工具软件一大堆，著名的有 Nmap、Nessus，OpenVAS 什么的，应该都玩过。

6.伪装攻击 Masquerading Attacks

①IP 欺骗 IP Spoofing

很简单，防范方法是在每个网络的边缘配置过滤程序，确保数据包满足以下标准：

*内部 IP 地址的包不能从外网进入。

*外部 IP 地址的包不能从内网出去。

*私有 IP 地址的包不能过路由器。

②会话劫持 Session Hijacking

会话劫持攻击指的是攻击者中途拦截已授权用户与资源之间的通信数据，然后使用劫持技术接管这个会话并伪装成已授权用户的身份。如：

*捕获客户端与服务器之间身份验证的详细信息，并使用这些信息伪装成客户端的身份。

*欺骗客户端，使其认为攻击者的系统是与之通信的服务器，并在客户端与服务器建立合法连接的时候作为中间人（代理），断开服务器与客户端的连接。

*使用没有正常关闭连接的用户的 cookie 数据访问 Web 应用程序。

7.内存重用（客体重用）

内存被重新分配后，要清空被覆写。

其它还有：陷门/后门/维护钩子等，好多。

五、软件保护机制（必考）

1.可信计算基

将安全内核和引用监视器关联在一起的术语是可信计算基(TCB)。TCB 是计算机系统内所有硬件，软件和固件的集合（组合体），它包含了该系统负责支持安全策略和对象隔离的所有元素。当 TCB 被启用后，该系统被认为具有可信路径并带有可信 shell。可信路径是在用户或程序与 TCB 之间的通信信道。TCB 负责提供需要的保护机制确保可信路径不能以任何方式受到破坏。可信 shell 意味着任何 shell 或通信信道内发生的活动，与信道隔离并且不能由不可行方或实体，无论是从内部还是外部进行交互。

TCB 的特性有：

*实施主体对客体的安全访问功能；

*抗篡改的性质；

*易于分析与测试的结构；

*安全保护能力主要取决于 TCB；

*基于 TPM 实现机密性，不管可用性。

①引用监视器 Reference Monitro

引用监控器/基准监视器，是一个抽象概念，但也可能有一个引用验证器，它通常运行在安全内核的内部并负责执行对对象的安全访问检查，操作权限，和生成任何的安全审计结果消息。换句话说，引用监控器被认为是一个抽象机器，其调解或控制，主体(用户)对客体(数据或资源)的所有访问。引用监控器采取行动以保证任何主体试图访问任何客体都要有适当的权限这样做，以便保护客体不受不良角色未授权访问的企图。安全内核真正地实现了引用监控器的概念。

引用监视器的**任务**：

根据访问控制数据库，对主体对客体的访问请示做出是否允许的裁决，并将该请示记录到审计数据库中。注意：引用监视器有动态维护访问控制库的能力。

引用监视器的**特性**：

执行主体到对象所有访问的抽象的机器；

必须执行所有验证策略，能够在修改中被保护，能够恢复正常，并且总是被调用；

处理所有主体到客体抽象机。

引用监视器必须满足的 3 个**条件**：

隔离、完整性、可验证。

You need Isolation, because it can't be of public access, the less access the better. It must have a sense of completeness to provide the whole information and process cycles. It must be veriable, to provide security, audit and accounting functions.

②安全内核 Security Kernel

负责实施系统安全策略的软件和硬件的组合体。

安全内核是由所有的 TCB(软件，硬件，和固件)组件构成且它负责建立和执行引用监控器。安全内核负责执行安全策略。它是一个引用监控器机制严格的实现。内核操作系统的架构通常是分层的，并且内核应该在最低且最原始的水平。它是操作系统的一小部分，所有对信息的引用和所有授权的改变都必须通过它执行。内核实现根据安全策略建立的对象之间的访问控制和信息流控制。为了安全，内核必须满足 RM 三个基本条件（和引用监控器的要求一样）：

*完整性：所有对信息的访问，必须经过内核

*隔离：内核本身必须防止任何类型的未授权访问

*可验证性：内核必须被证明符合设计规范

TCB 中使用的产品的安全能力可以通过各种评价标准进行验证，如较早的可信计算机系统评价标准(TCSEC)和当前的通用准则标准。

③处理器特权状态

处理器特权状态保护处理器和它执行的活动。最早的实现的方法是在一个寄存器中记录处理器的状态，只有当处理器在特权状态下操作时才能改变它。像 I/O 之类的指令请求被设计为包含一个对这个寄存器的引用。如果寄存器不是在特权状态，指令就被终止。例如，intel 处理器防止对系统代码和数据的覆盖，尽管这些保护很少被直接使用。特权机制应防止从较低特权到更高特权的内存访问(程序或数据)，但只有当控制被调用且在软件中适当地管理时。特权级别通常参考环结构。为了说明这一点，许多操作系统使用两种处理器的访问模式：

*用户模式(或进程、问题、程序)

*内核模式(或特权、监管)

用户应用程序代码运行在用户模式，并且操作系统代码运行在内核模式。特权的处理器模式被称为内核模式。内核模式允许处理器访问所有的系统内存，资源，和 CPU 指令。

应用程序代码应在非特权模式(用户模式)运行并且有一个受限的可用接口，受限的系统数据访问，并且不能直接访问硬件资源。操作系统有比应用软件更高的特权级的一个优点是出问

题的应用软件不能破坏系统的运作。当一个用户模式的程序调用系统服务(例如从存储中读一个文档)，处理器缓存这个调用并将这个调用请求切换到内核模式。当这个调用完成后，操作系统把调用切换回用户模式，并允许用户模式程序继续运行。在最高安全操作策略下，操作系统和设备驱动程序运行在 0 环级，也称为内核级或系统级特权。在这个特权级，程序可以做什么没用限制。因为在这个级别的程序访问不受限制，用户应该关注包含敏感信息的机器上设备驱动程序的来源。应用和服务应该工作在环 3 级，也被称为用户级或应用级特权。需要注意的是，如果一个这个级别上的应用或服务失败，一个捕获屏幕将出现(也称为一般性保护错误)，其可以被关闭且操作系统并不关心。把服务和常规的应用运行在相同特权级的决定是基于这样的思想，如果服务被捕获，操作系统应该继续操作。

④缓冲区溢出的安全控制

不当的边界检查导致恶意输入到程序；必须由程序员更正或直接打系统内补丁。所以，输入的参数必须要检查合规，操作系统也要提供缓冲区管理机制，如进程隔离和内存保护。

另一个与特权状态相关的问题被称为无效的参数检查，这导致了缓冲区溢出。一个缓冲区是由对程序的输入不正确(或缺乏)边界检查造成的。本质上，程序未能发现给一个分配的内存空间的数据是否太多。因为当程序运行的时候被加载到内存，当溢出发生时，数据必须去某些地方。如果那些数据恰好是被加载的可执行恶意代码，它可以像那个程序一样运行，或对运行环境做出其他改变，其可被攻击者利用。缓冲区溢出必须由程序员或通过直接打内存补丁修正。它们可以被检测到并修正，通过逆向过程(反汇编程序)并检查应用的操作。硬件状态和其它硬件控制能使缓冲区溢出变得不可能，虽然企业很少指定此级别的硬件。边界强制和正确的错误检查也将停止缓冲区。

⑤中断

可以实现进程隔离。计算机内的进程必须互相隔离的需求必须被管理，以确保它有效地和全面地发生，没有例外。操作系统就是这样的程序，它的执行确保进程隔离发生并且它与 CPU 共同通过中断和时间分片的使用来执行进程隔离。中断的使用允许操作系统确保一个进程被给予充足的访问 CPU 的时间，当需要执行它所需的功能时，但它也确保进程不会停留过久的欢迎且锁定其它进程的执行需要的资源。

中断是单片机实时地更紧密地处理外部事件的一种内部机制。“没有中断就没有操作系统”。中断处理的时刻一定是在一条指令执行结束，转入下一操作时（准备处理另一个程序了）。中断的处理：发现中断请求，指令控制器中止正在运行的程序，保存该程序的运行现场（当前状态）；根据中断信号从待定位置启动中断处理程序（操作系统提供）处理中断；处理完了恢复前面的程序或者处理下一个中断请求。中断的产生：各种软硬件的中断信号。

为了执行进程隔离的概念，操作系统可以使用以下任何一种方式：

*对象封装，可隐蔽其内部工作流程和数据。

*共享资源的时分复用，允许操作系统，以提供结构化的访问需要根据一个严格管理的时间表使用资源的进程。

*命名区分，每进程被分配唯一的标识即进程 ID，或 PID。

*虚拟地址映射，不直接访问物理内存。

⑥内存管理器

最重要的就是运用上面讲的虚拟地址映射。

它是操作系统用来跟踪不同类型的内存是如何被使用，分配和释放进程运行需要的不同类型的内存，强制访问控制以确保进程只能与它们自己的内存段交互，并在需要时，管理 RAM 中的内存内容交换到硬盘。有五个职责：

*重定位：当需要时，在 RAM 和硬盘之间移动或交换内容并给应用提供指针，如果它们的信息已经被移动到内存中的不同位置。

*保护：提供内存段的访问控制并且限制应用只能与分配给它们的内存段交互。

*共享：使用共享内存段，允许有不同访问级别的多个用户与一个应用或进程交互，同时在进程之间运行和执行完整性和机密性控制。

*逻辑组织：所有类型的内存分段管理，在一个抽象的水平提供一个寻址方案，并允许共享像 DLL 程序那样的软件模块。

*物理组织：为了分配内存，分段所有的物理内存空间。

内存管理过程还有一个附加部分需要讨论，即寄存器的使用。寄存器允许操作系统确认一个进程只能与内存管理器分配给它的已定义的内存段交互。CPU 使用两种类型的寄存器来识别内存地址：

*一个基寄存器用来标识分配给进程的开始地址

*一个限制寄存器用来标识分配给进程的结束地址或信息破坏。

一个 CPU 将创建一个或多个线程来执行一个进程。线程是进程产生的一组指令的集合，以运行它执行其被要求执行的特定活动。CPU 使用线程以允许进程执行动作，通过引用需要执行的指令和数据驻留在内存中的地址。CPU 将地址与基和限制寄存器进行比较，以确保进程请求的访问在分配给进程的允许的内存空间之内，而不是之外或在一些其它被保护的内存空间。内存保护关注对主内存的访问控制。当几个进程在同时运行时，需要保护一个进程的内存防止被另一个进程未授权访问。因此，必须对内存进行分段，以确保进程的本地内存不会相互干扰且确保公共内存区域不受未授权访问。这个扩展超越了运行在主计算机内存中的应用：操作系统可以使用辅助内存(存储设备)，给出一个较大的主内存池的假象，或者它可以将主内存在用户间分区，这样每个用户都看到一个内存比真实机器上的内存小的虚拟机。这种情况下可能需要一些额外的控制。

⑦内存保护方法（考点）

有四种方法来提供内存保护，这样没有用户进程可以无意地或故意地破坏另外一个进程的地址空间或操作系统本身。

*第一种方法，确保由内核模式系统组件使用的所有系统范围内的数据结构和内存池，只能在**内核模式**下访问。因此，用户模式的请求不能访问这些内存页。如果他们试图这样做，硬件将产生一个错误，随后内存管理器将产生一个访问冲突。在早期的 Windows 操作系统中，例如 Windows 95 和 Windows, 98，系统地址空间中的某些页可以由用户模式写入，从而使一个错误的应用程序破坏关键的系统数据结果并导致系统崩溃。一个硬件抽象层(HAL)的实现以及改进的内存管理技术已经消除了此问题，其结果是，由于这个原因，更近的基于 Windows 的操作系统不会遇到这种相同类型的行为，例如桌面系统中的 Windows 7 和 8 以及服务器方面的 Windows Senver2008 和 2012。（确保所有的全系统的数据结构和存储器所使用的内核模式系

统组件池可以访问公在内核模式。）

*在第二个方法中，每个进程有一个单独，私有的地址空间被保护不受属于其它进程的请求的访问，也有极少数例外。每次当一个请求引用一个地址时，虚拟内存硬件，与内存管理器一起,干预和转换这个虚拟地址到物理地址。这种控制机制被称为**地址空间布局随机化**(ASLR)。ASLR 在很多操作系统平台实现，并允许内存管理器有效的改变，或随机的，进程使用的内存地址空间地址，其在一个连续的基础上执行。因为像 Windows 7, Windows 8/8.1，和 OpenBSD 这样的操作系统，控制虚拟地址如何转换，一个进程中运行的请求不会不恰当地访问一个属于另外一个进程的页面。（第个过程有一个单独的，专用地址空间从属于另一个任何请示被访问受保护过程中，有少数例外。）

*在第三种方法中，大多数现代处理器提供某些形式的硬件或软件控制的内存保护，例如读或写访问。虽然这种保护机制的实现根据制造商所有不同，它通常被称为**数据执行保护**(DEP)。提供的保护的类型取决于处理器。例如，一个内存保护选项是 PAGE_NOACCESS。在这个区域，一个读取，写入，或执行代码的试图，就会发生访问冲突。DEP 有使某些系统内存区域对进程的执行不可用的能力，通过标记它们为不可用来实现。这有双重好处，减少由内存管理器管理的可用内存区域，同时减少可以提供给一个进程在其内执行的可用内存区域。这允许操作系统进一步优化性能，加快交易速度，以及减少攻击者为了执行攻击可以获取访问的可用内存空间。（大多数现代处理器提供某种形式的硬件或软件控制的存储器保护功能，如读或写访问。）

*第四种保护机制使用**访问控制列表**来保护共享内存对象，当进程试图打开它们的时候，强制它们接受安全检查。另外一种安全功能涉及映射文件的访问。为了映射一个文件，执行请求的客体(或用户)必须至少有对底层文件对象的读取访问权限，否则操作将失败。（使用访问列表来保护共享内存对象，迫使他们接受安全检查时，流程试图打开它们。）

⑧隐蔽信道控制（必考）

隐蔽信道或约束问题是一个没有被安全措施控制的信息流。它是一个通信渠道，允许两个合作的进程，以一种违反系统安全策略的方式，传递信息。即使存在保护机制，如果未授权信息用信号机制或其它对象进行传递，那么一个隐蔽信道就可能存在。在应用安全中使用的标准例子是这样一个情景，一个进程可以被一个程序启动或停止，这个进程的存在可以被另一个应用检测到。这样，这个进程的存在可以用于，随着时间的推移，发出信号信息。唯一要关注的信道是违反安全策略的那些；并不必关注那些与合法通信路径并行的信道。虽然每一类隐蔽信道都有区别，但有一个共同的条件：通过通道发送和接收的对象必须能访问共享资源：

*第一步是识别任何潜在的隐蔽信道；

*第二步是分析这些信道以确定一个信道是否真实地存在；

*接下来的步骤是基于人工检查和适当的测试技术，以验证信道是否创建了安全关注。

⑨编程语言支持

提供程序安全执行的另一个方法是使用一个更安全的编程语言(也被称为强类型)，比如 Java。类型安全的语言或安全语言是一个程序，它永远不会在某些方面出错。确保数组在边界之内，指针总是有效的，并且代码不能违背变量的类型(例如把代码放在字符串中，然后执行它)。从安全的角度看，没有指针很重要。通过指针访问内存是导致 C 或 C++程序漏洞(错误)

和安全问题的一个主要原因。Java 在内部执行了检查，称为静态类型检查，它检查是否一个操作在执行的时候获得的参数的类型始终正确。

强类型就是编程的语言必须满足高标准的规范要求，如果不是，则被称为弱类型。

B.3 配置管理（CM）作为安全编码的一个方面

对于软件，配置管理(CM)是指监控和管理对程序和文档的变更。

目标是保证完整性，可用性，和所有系统组件的正确版本的使用，例如软件代码，设计文档，文档，和控制文件。配置管理涉及对系统所做的每一个变更。这包括所有变更的控制，核查，和审计。

*第一步是确定所做的所有变更。

*控制当对某些类型的文档的所有变更发生时，必须被评审且由授权人员进行批准。

*核查是记录和报告通过任何变更流程对软件或硬件的配置。

*审计允许完成的变更被验证，尤其是确保任何变更不会影响已经建立的安全策略或保护机制。还有变更计划管理和信息保护管理就不说了。

1.配置管理的类型：

①并发管理(concurrency management)：确保多人从同一库中导出的文件是完全一致的。

②版本管理(versioning)：记录、跟踪、保持文件的各个版本，支持回滚。

③同步控制(synchronization)：在工作需要时同步库中的所有或部分版本。

2.配置管理的过程：

①识别(Identification)：识别并记录每个配置项的功能和物理性。

②控制((Control)：控制对配置项的变更，从软件库发布配置项的版本。

③状态记录(Status Accounting)：记录变更的处理过程。

④审计(Audit)：控制配置管理过程的质量。

3.软件托管 Software Escrow（考点）

在第七域 F.2 章节讲过了。软件托管协议 Software Escrow Arrangements 是一种特殊的工具，可以对公司起到保护作用：它避免公司受软件开发商的代码故障的影响，以便为产品提供足够的支持，还可以防止出现由于开发商破产而造成产品失去技术支持的情况。在软件托管协议下，开发商将应用程序源代码的副本提供给独立的第三方组织机构。然后，第三方用安全的方式维护源代码副本备份的更新。这个经常考到，就是要找一个监理人来监督第三方的软件开发。如果软件开发商倒闭了，我还要用它的源代码里，只能找第三方来要了。

最知名的软件代码托管网站：GitHub。

B.4 代码仓库的安全

软件开发是一个庞大团队的高度协同工作的复杂工程。Github、Bitbucket、和 SourceForge 等代码仓库 Code Repositories（有的是开源仓库），可以用作软件代码的核心集中存储，提供版本控制、缺陷跟踪、网站托管、发布管理、通信等功能，以支持软件开发。

1.API keys

公共基础设施和 IaaS 服务提供商都提供了 API 接口来定制和使用基础服务。当然，这些

服务是收费的，用于创建服务器的 API key 绑定服务器到一个特定的用户帐户(和信用卡)。如果开发人员编写代码，包括了 API keys ，然后上传到一个公共的代码仓库，你的收费服务很可能被黑客利用。

2.GitHub 的安全措施活动

GitHub 是很重要的代码管理系统（托管），它提供的安全措施有：

①物理安全，数据中心的访问仅限于数据中的技术人员和批准的 GitHub 员工，有严格的访问控制和审计。

②系统安全，系统有完善的安防系统，使用加固、打过补丁的操作系统；专用的防火墙和 VPN 服务；专用的入侵检测；分布式拒绝服务(DDoS)攻击缓解服务等。

③运行安全，所有敏感信息、的安全文档销毁策略；完全文档化的变更管理流程。

④软件安全，我们在 GitHub 聘请了一个 24/7/365 服务器专家团队。

⑤通讯，所有和 GitHub 交换的私有数据总是通过 SSL 传输，通过 SSH 认证。

⑥文件系统和备份，每一行代码至少保存在三个不同的服务器上，包括异地备份。

⑦员工访问，没有任何 GitHub 员工可以访问过私有代码库除。

⑧维护安全，使用速度限制来防范暴力攻击，使用双因素认证。

⑨信用卡安全，不存储任何卡片的信息。

B.5 应用程序编码接口的安全

API 的安全问题主要涉及：

用户认证、用户授权、加密、防止未经授权的访问、问责制和审计。

分层方法是最经典的安全控制方法，互联网访问经常用到，一般分三层：

表示层、业务逻辑层、数据层。

不过数据库管理系统本身提供的安全特性，因为使用了中间层（中间件），而丢失、无效。业务逻辑层建立的是“虚表”。因为有“中间件”，本身就保护了对数据库的攻击。

1.应用编程接口 API/ Application Programming Interfaces

为了使这些跨站点/跨系统的软件功能正常工作，每套独立软件都要提供应用编程接口，允许程序开发人员通过函数调用来直接与底层服务进行交互。应用编程接口是物联网(IoT)的连接器，允许我们的设备可以互相通讯。与此同时，然而，API 是互联网“未知的，看不见的力量”，因为最终用户并不知道它们的存在。然而，API 无处不在。API 必须被管理和保护。

2.表述性状态转移(REST)representational state transfer API（考点）

REST 是通过 URL 路径元素表达系统中的特定实体的方法；REST 不是一个架构，但它是在 Web 上建立服务的一个架构风格。REST 允许通过简化的 URL 与一个基于 Web 的系统交互，而不是复杂的请求体或 POST 参数从系统请求特定项。对于涉及 API 安全的安全专业人员来说，广泛使用的 REST API 才是真正的关键挑战的核心。今天无处不在使用 REST API。关于 web 服务，符合 REST 约束的 API 称为 REST 风格(RESTful)。

3.基于 REST API 安全建议（建议性的东西都不用细读，一般不考的）

①使用与你的组织部署的任何 web 应用一样的安全机制部署你的 API；例如，如果你是在 web 前端过滤 XSS，你也必须为你的 API 这样做，最好用同样的工具。

②不要创建和实现你自己的安全解决方案。使用框架或现有的库，其已经过同行评审和测试。不熟悉设计安全系统的开发者经常产生有缺陷的安全实现，当他们试图自己做的时候，结果他们使他们的 API 容易受到攻击(记住 Tesla 讨论)。

③除非你的 API 是免费的，只读的公开的 API，不要使用单一的基于键的认证。这是不够的。你应该添加一个密码要求。

④不要传递未加密的静态密钥。如果你正在使用 HTTP 且通过线路发送，那么请确保你始终加密它。

⑤理想的情况下，使用基于散列的消息验证码(HMAC)，因为它是最安全的。使用 SHA-2 和以上；避免用 SHA 和 MD5 因为已知的漏洞和弱点。

4.认证选项

就是实现 REST 安全的 3 种方法，有三种主要方式你需要熟悉：

①基本身份认证 w/TLS。基本身份认证是三个其中最早建立的，因为大多数情况下它可以在没有额外库下实现。实现基本身份认证需要做的所有事情通常已经包含在你的标准框架或语言库中。基本身份认证的问题是它是基本的，并且它只提供了可用的通用协议最低级别的安全选项。没有高级选项使用此协议，所以你只是发送一个 Base64 编码的用户名和密码。如果没有使用传输层安全协议(TLS)。决不能使用基本身份认证，因为用户名和密码的组合可以很容易的被解码。

②Oauth1.0。是这三个中最常见的协议。该协议使用一个加密签名(通常是 HMAC-SHA 值，它组合了令牌秘密，随机数，和其它基于请求的信息。OAuth 1 巨大的优势是你从不直接通过线路传递令牌秘密，从而彻底消除了可能有人看到传输中的密码。这是三个协议中唯一可以在没有 SSL 下安全使用的协议，如果传输的是敏感数据，你还应该使用 SSL。不过，这个安全级别是有代价的：产生和验证签名可能是个复杂的过程。你必须按照严格的步骤，使用特定的散列算法。这实际上已经不是问题，因为每一个主流编程语言都已经提供了库为你处理这些。

③Oauth2.0。现行规范中删除了签名，所以你不再需要使用加密算法来创建、产生和验证签名。所有的这些加密现在都是由 TLS 处理，这是必须的。Oauth2 的库没有 Oauth1.0a 的库那么多，所有集成这个协议到你的 API 可能更具挑战。

B.1 章节讲单点登陆时也提到了 Oauth，它可以用于单点登陆。

此外，像密钥管理互操作系统(KMIP)V1.1 这样的解决方案；客户端证书和 rHTTP 摘要也可作为创建安全方案的的可能选项来查看。

5.OWASP REST 安全备忘单

当检查基于 REST API 安全需求和关注时，另外一个资源可以考虑的是 OWASP REST 安全备忘单。一个安全备忘单例子是：

RESTful web 服务应使用基于会话的身份认证，通过一个 POST 建立一个会话令牌或使用一个 API 密钥作为 POST 体的参数或作为 cookie。用户名和密码，会话令牌，和 API 密钥不应出现在 URL 中，因为这可能在 web 服务器日志中捕获并使它们内在的有价值。

6.Web 服务的通信

面向服务的软件架构 SOA 常被考到，相关的技术协议都要了解。

①SOAP 简单对象访问协议(Sirrple Object Access Protocol)

用来描述传递信息的格式。SOAP 是交换数据的一种协议，是一种轻量的、简单的、基于 XML 的协议，用于在 WEB 上交换结构化的和固化的信息。可以和许多因特网协议和格式结合使用，包括超文本传输协议(HTTP)，简单邮件传输协议(SMTP)，多用途网际邮件扩充协议(MIME)等。它还支持从消息系统到远程过程调用(RPC)等大量的应用程序。SOAP 使用基于 XML 的数据结构和超文本传输协议 HTTP 的组合定义了一个标准的方法来使用 Internet 上各种不同操作环境中的分布式对象。

④Web 服务描述语言 **WSDL**(Web Services Description Language)

用来描述如何访问具体的接口。

②统一描述 **UDDI**(Universal Description, Discovery and Integration)

用来管理、分发、查询 web service。

③XML(Extensible Markup Language)，不说了。

④HTTP，不说了。

C.评估软件安全的有效性

1.认证与认可

前面讲过很多次了。

认证是指技术评估或评价信息系统在它们的操作环境中的安全合规性：用户和管理者的背书，系统/应用符合他们的功能需求，并且在大多数情况下，背书的独立的验证。

认可或授权过程审查认证(或评价)信息，并授予官方的授权将信息系统投入操作使用：它是高级管理人员的正式批准。

2.风险管理框架

传统的认证和认可的过程已经转变为一个六个步骤的风险管理框架（RMF）。

风险管理过程改变了传统 C&A 的焦点，从一个静态的，过程性的活动变为更加动态的方法，提供了更加高效地管理信息系统相关的安全风险的能力，在一个高度多样化的环境：复杂和尖端的网络威胁，日益增加的系统漏洞，和快速变化的任务。

C.1 审计和日志的变更

1.日志

日志是已经发生在计算机系统上的行为和事件的记录。

*提供了一个清晰的视图：谁拥有一个进程，发起了什么行为，什么时候发起的，该行为在哪儿发生的，以及为什么进程执行。

*主记录是系统和网络的活动的保管者。

*对抓住解释，发生了什么以及为什么在事件中安全控制失效了的相关的信息非常有帮助。

2.审计

为了企业的最佳利益，应有适当的审计策略存在，有效地以日志的形式收集关于网络和系统中发生的关键事件的信息，并适当的管理它们。这些信息、是关于事件的，以日志的形式获得，将使所有感兴趣的各方，例如高层管理人员以及网络和系统管理员，去了解和评估：

*建立基线的需要

*不同服务器和系统的性能

*应用的功能和操作问题

*有效的检测入侵企图

*取证分析

*遵守各项法律法规

3.信息的完整性，准确性，和审计

*信息的完整性：应该使用流程来比较或调和处理了什么和什么应该被处理。例如，控制可以比较总和或检查序列号。这将检查是否对正确的数据执行了正确的操作。

*信息准确性：为了检查输入的准确性，数据确认和验证检查应纳入相应的应用。字符检查比较输入的字符串和期待的字符类型，例如数字或字母。有时也称为合理性检查。范围检查验证输入的数据与预定义的上限和下限。关系检查比较输入数据与主记录文件中的数据。合理性检查比较输入数据与一个预期的标准，合理性检查的另一种形式。交易限额检查输入数据与行政上对特定交易设定的最高限额。

*信息审计很重要，因为漏洞存在于软件的生命周期中；攻击会就有发生的可能性。审计过程协助检测任何异常行为。一个安全信息系统必须提供一个授权人员，有能力审计任何行为，其可能潜在地引起访问，破坏，或以某种方式影响敏感信息的发布。

审计的水平和类型取决于已安装软件的审计要求和数据的敏感性，其在系统中处理和存储。关键因素是审计数据提供了发生了什么类型的未授权活动和谁或什么进程执行了这个活动的信息。

C.2 风险分析与缓解

1.基础知识

风险的内容还是看第一域吧。

风险：具有发生的可能性并对发生风险的项目有一个正面或负面的影响的一个事件。一个风险可能有一个或多个原因，并且如果发生时，造成一个或多个影响。

风险管理：是一个持续的过程，贯穿项目的生命周期。它包括风险管理规划，识别，分析，监控，和控制的过程。在任何时候一旦新的风险被识别，很多的以上这些过程在项目生命周期中会被更新。风险管理的目标是减少对项目负面的事件发生的可能性和影响。另一方面，任何可能有正面影啊的应该加以利用。

风险识别：一般都是在项目之前启动的，在项目的生命周期中，随着项目成熟风险的数目也在增加。当一个风险被识别后，它将首先被评沽发生的可能性，对进度，范围，成本，和质量影 An 的程度，然后进行优先级排序。

优先级：风险事件可能影啊一个或多个影响类型。风险优先级的分配基于：

*发生的可能性

*影响类别的数量

*它们对项目影响的程度(高，中，低)

记录风险：所有识别的风险应该进入一个风险登记册并作为风险声明的一部分记录。作为记录风险的一部分，另外两个重要项需要解决：

*第一是可用于减轻事件发生的可能性的减缓步骤

*第二是应急计划，在事件发生前或发生时应该采取的一系列的活动

减缓和应急计划：减缓行动经常需要成本。有时减缓风险的成本可能超过假定风险和产生的后果。在决定建立一个应急计划前，针对减缓策略的成本评估每个风险的可能性和影响是非常重要的。风险发生前实施的应急计划是防范活动，旨在降低影响或完全消除风险。风险发生后实施的应急计划通常只能减轻影响。

2. 最佳实践

这些通用的最佳实践包括以下：

①使用变更控制过程。

②阅读所有相关文档。

③测试。服务包和补丁程序在部署到生产之前，必须在有代表性的非生产环境进行测试。

④有一个工作备份和生产停机时间计划。

⑤必须有回退计划。允许系统和企业返回到失败的实施之前的状态。

⑥预警服务台和关键用户组。

⑦首先瞄准非关键服务器：如果所有的测试在实验室环境中都成功，先从非关键服务器开始部署，如果可能的话，然后在服务包已经在生产环境运行 10-14 天后，再向主服务器部署。

3. 风险管理工具

包括石川图（因果图），P-图，初步危害分析/预先危险分析(PHA)，失效模式与影响分析(FMEA, Failure Modes and Effect Analysis)，故障模式、影响及危害性分析(FMECA)，危害分析与关键控制点(HACCP)等等。

C.3 测试与验证

作为开发过程的一部分，在分发任何软件之前必须彻底测试它。

测试和验证是不同的，测试是发现问题；验证相关于审计，是确认问题被解决了。

1. 三种测试方法：

①白盒测试：要检查一个程序的内部逻辑结构和一行行的代码，分析程序中潜在的错误。

②黑盒测试：从用户的角度提供输入场景并检查输出，只验功能不看代码。

③灰盒测试：灰盒测试结合了两种方法，是流行的软件验证方法。

2. 两种类型测试：

①静态测试：分析源代码或编译后的应用程序，并运行它。一般用工具软件查缓冲区溢出。

②动态测试：在运行环境中评估软件，是正式部署前的唯一、必然测试手段。

另一种分类方法：

①盲目/单盲测试：评估人员只能利用公开可用的数据，而网管人员将知道有这种测试。

②双盲测试/隐蔽评估：评估人员只能利用公开可用的数据，网管和安管不知道有测试。双盲测试能够评估网络的安全级别以及员工的响应能力、日志监控和上报流程，从而更加现实地说明了发起某种攻击的成功或失败几率。

3. 软件功能测试的类型：

①单元测试(Unit testing)：验证受控环境中的单个组件的数据结构、逻辑以及边界条件。

②集成测试(Integration testing)：验证组件是否按照设计规范中那样协同工作。

③验收测试(Acceptance testing)：确保代码满足客户需求。

④回归测试(Regression testing)：系统变更后重新测试确保其功能性能以及安全达标。

4.软件安全测试的类型：

①模糊测试(Fuzzing testing)：发送复杂/随机的数据给软件来引起软件的错误，主要用于识别缓存溢出、DOS、注入、验证错误以及其他可能导致软件死机、崩溃或发生各种错误。

②脆弱性扫描(Vulnerability scaning)：通过自动化工具检查程序的主要错误，如强类型语言的错误、开发和配显错误、交易序列错误(transaction sequence faults)、映射出发条件(mapping triggerconditions)等，通常在扫描完后需要手工进一步的核查。

③人工测试(Acceptance testing)：通过人员的经验和直觉来分析程序，通常使用计算机技术来判断，测试人员能定位设计错误，如逻辑错误。包括渗透测试。

④动态分析(Dynamic analysis)：及时的分析正在运行的程序，一般是在静态分析之后，程序的基本问题都被解决完后执行。

5.代码签名 code signing

代码签名是一种安全技术，可以用来确保代码完整性，确定谁开发了一段代码，并确定开发者预期使用这段代码的目的。所有类型的代码都可以被签名，包括工具，应用，脚本，库，插件，和其它“类代码”的数据。代码签名不是数字版权管理(DRM)或复制保护技术，它也不能保证代码没有安全漏洞。代码签名有三个不同的目的，它可用于：

①完整性。确保一段代码没有被修改

②来源。鉴定代码来自特定的源(开发者或签名者)

③代码的用途。为了特定的目的，确定代码是否可信赖，例如，访问一个特定项

为了使签名代码能实现这些目的，一个代码的签名由三部分组成（考点）：

①一个印章/信封 seal，它是代码各个部分的校验和或哈希的集合，例如标识符，主可执行文件，资源文件，等等。印章可用于检测对代码和应用标识符的修改。

②一个数字签名，它签名印章以保证它的完整性。签名包含了信息，可以被用来决定谁签名了代码和是否签名是有效的。

③一个唯一的标识符，可以用于识别代码或代码属于哪一个组或类别。这个标识符可由签名者明确地提供。(标识符+印章)=>签名，①+③=>②

6.回归和验收测试

只要开发者改变或修改他们的软件，即使一个很小的调整可能也会有意想不到的后果。

①回归测试（考点）

回归测试是指对现有的软件应用进行复核式检查，以确保之前的某些变更行为并没有破坏其功能或安全性。执行回归测试时，主要考虑的是足够的覆盖范围和不会浪费时间。

②使用测试库

最有效的回归测试的方法是基于开发一个测试库，由标准测试用例组构成，它可以在任何有程序的新版本构建时运行。建立一个测试库最困难的部分涉及到包含哪一个测试用例。很多敏捷环境使用工作流的做法，例如 XP(极限编程)，RUP(统一软件开发过程)，或者 Scmm 使用回归测试作为一个动态的，迭代的开发和部署计划的一个重要方面。

③验收测试

验收测试是执行的一个正式测试，以确定一个系统满足其验收标准且使用户可以决定是否接受该系统。这在最初被称为功能测试，它不同于单元测试，通常在一个完整的系统上进行。

④敏捷开发环境中的验收测试

在敏捷软件开发中，验收测试/标准通常由业务用户创建并使用业务领域的语言表达。这些是高层次的测试，以验证一个用户故事或故事集的完整性，它被在任何的冲刺/迭代的过程中被“执行”。理想情况下，这些测试通过业务客户，业务分析员，测试员，和开发者合作创建的。重要的是这些测试包括业务逻辑测试同时也包括 UI 验证元素。业务客户(产品所有者)是这些测试的主要人员。当用户故事通过他们的验收标准后，业务所有者可以放心认为开发者在朝着正确的方向前进。

D. 评估采购软件的安全影响

当组织购买软件时，安全专业人员必须了解软件的合理配置以满足安全目标，还必须修复安全漏洞。在 SaaS 环境下，大多数安全责任在供应商侧，但甲方的安全人员也要负责监控供应商的安全，包括审计、评估、漏洞扫描和其他措施等。

1. 软件保障(SWA)

根据美国国家安全系统委员会国家信息保障(IA)法案，CNSS 指令 4009 号，2010 年，4 月 26 日，69 页：“软件保障是对软件信心的水平，其没有漏洞，无论是故意设计到软件中还是意外地在其生命周期中插入的，并且它以预期的方式工作。”SWA 是至关重要的，因为急剧增加的业务和使命的风险是由于软件不能按预期执行并可以被利用引起的。为了确保业务运作和关键基础设施中的关键资产的完整性，软件必须可靠和安全。

2. SwA 阶段

SwA 可以围绕着一个通用的采购过程的主要阶段组织。主要的阶段是：

规划—合同—监控和验收—后续

①计划/规划阶段 Planning

这个阶段开始于：需要确定采购的软件服务或产品，识别潜在的替代软件的方法，并确定这些替代品相关的风险。

②招标/合同阶段 contracting

这个阶段包括三个主要的活动：*创建/发出邀约；*评估供应商；*落实谈判。

③监控和验收阶段 monitoring and acceptance

监控供应商的工作并根据合同接受最终交付的服务或产品。

④后续阶段 follow on

维护软件(该过程通常被称为维持)。

第九域　考试重难点归纳

A. 新旧大纲对比

具体不列举了，现在的学习资料都是新大纲的，相关对比在“九阴真经”之 CBK 的内容里有详细的文档，而且在 AIO7 英文版里，把新增内容的标签都加粗了。如果最初复习是以 AIO6 为主的，需要补充学习新增的内容。有的培训班到 2017 年了，用的资料居然还以老大纲的十个域的内容和习题为主，讲师还没有整理出成体系的新教材。

B. 官方教材要点汇总

CBK、OSG、AIO 这 3 本权威教材每个章节后面列举的知识要点，是必须掌握的，可以对照自查，这里不复制粘贴了。

推荐 2 本 2016 年最好的英文辅导书，绝对的宝典，完成是针对考试的要点整编和应试技巧，只是来不及翻译了，都收录在“九阴真经”之 OSG 里了，自己看吧。分别是：03_CISSP Study Guide, Third Edition-2016,最新版英文核心辅导材料；和 04_CISSP Comprehensive Review Notes-2016,最新版英文学习笔记。前者就像是考试真题的出题者在介绍考试重点；后者则是像学霸的必考要点学习笔记。

C. 法规标准汇总

几乎所有的考试内容都是从某个法规、标准、指南中引用来的。CISSP 不考某国的法规标准，只考国际的，不过美国、欧洲的一些代表性典型基础法规也会考到。先熟悉相关组织机构：

1. 美国的

①**NIST**（National Institute of Standards and Technology），美国国家标准与技术研究院。CISSP 最重要的理论来源，基本完全引用了它的术语。

②**NSA**（NationalSecurityAgency），美国国家安全局。

③**DOD**（Department of Defense），美国国防部。

2. 其它的

①**ISO**（International Organization for Standardization），国际化标准组织。目前世界上最大、最有权威性的国际标准化专门机构。

②**IEC**（InternationalElec－trotechnicalCommission），国际电工委员会。成立于 1906 年，负责有关电气工程和电子工程领域中的国际标准化工作，总部设在瑞士日内瓦。

③**ITU**（InternationalTelecommu－nicationUnion），国际电信联盟。由法、德、俄等 20 个国家在巴黎会议上为了顺利实现国际电报通信而成立的国际组织。ITU 的实质性工作由三大部门承担：国际电信联盟标准化部门、国际电信联盟无线电通信部门和国际电信联盟电信发展部门。

④**IEEE**（Institute of Electrical and Electronics Engineers），电气和电子工程师协会。国际性的电子技术与信息科学工程师的协会，全球最大的非营利性专业技术学会。

⑤**BSI**（British Standard Institution），英国标准协会。举世闻名的，集标准研发、标准技术信息提供、产品测试、体系认证和商检服务五大互补性业务于一体的国际标准服务提

供商，面向全球提供服务。

⑥EU（European Union）欧盟。根据 1992 年签署的《欧洲联盟条约》（也称《马斯特里赫特条约》）所建立的国际组织，现拥有 28 个会员国。欧盟是世界上最有力的国际组织之一，在贸易、农业、金融等方面趋近于一个统一的联邦国家，而在内政、国防、外交等其他方面则类似一个独立国家所组成的同盟。

⑦ENISA（The European Union Agency for Network and Information Security），欧洲网络与信息安全局。

C.1 重要的系列法规

一、NIST SP 800 系列

NIST SP 800 是美国国家标准与技术研究院发布的一系列关于信息安全的技术指南文件(SP 是 Special Publications 的缩写），提供了可供参考的方法和经验。虽然 NIST SP 并不是强制性的法定标准，但已经成为美国和国际安全界得到广泛认可的事实标准和权威指南。截至 2011 年，NIST 访问控制系列已经出版了 17 个簇类、126 本信息安全相关的正式文件，形成了从计划、风险管理、安全意识培训和教育以及安全控制措施的一整套信息安全管理体系。

1.基础类

①SP 800-12（计算机安全介绍：NIST 手册，1995 年）

论述了计算机安全控制的益处以及其合理应用的条件，帮助读者理解计算机安全需求。

②SP 800-14（信息系统安全的公认原则和实践，1996 年）（**第三域**）

提供了机构用来建立和检查 IT 安全程序的基线，和管理各种事务的基础参考。

2.访问控制类

①SP 800-120（EAP 方法在无线网络访问身份验证的建议，2009 年）

描述了使用创建的密钥进行身份验证的安全需求。

②SP 800-103（身份凭证，第一部分本体论，背景和公式化，2006 年）

描述了身份凭证的本体论，通过 XML 架构的形式明确表示。

③SP 800-122（个人识别信息 PII 保密指南，2010 年）

帮助联邦机构保护个人识别信息的机密性。

④SP 800-73（个人身份验证接口）

⑤SP 800-76（生物识别数据规范的个人身份验证）

⑥SP 800-77（IP 协议(IPSec)虚拟专网 VPN 指南）

⑦SP 800-78-3（个人身份验证的加密算法和密钥规格 PIV，2010 年）

⑧SP 800-125（安全虚拟化技术指南）

3.意识培训类

①SP 800-100（信息安全管理指南/手册，2006 年）

从管理层面对意识和培训进行了描述，提供了信息安全规划各部分的概述，帮助建立和实施信息安全项目。

②SP 800-16（信息系统安全培训要求：基于角色和效能的模型）战术层面、针对政府。

③SP 800-50（建立信息安全意识和培训方案，2003 年）策略层面、针对企业组织。

4.认证认可&安全评估

认证认可和安全评估是以FIPS 200为基础，从测试和评估、身份验证、性能测量、安全控制措施评估等多个方面进行了规范。

①SP 800-115(信息安全测试和评估技术指南，2008年)

是关于信息安全评估基本技术的指南，描述了机构在进行评估时可能用到的技术测试、检测方法和相关技术，为评估人员在系统和网络上关于执行和潜在影响提供了深刻的理解。

②SP 800-53 Rev.3（联邦信息系统**安全控制措施评估指南**，2009年）（**第一域**）

在商业领域，审计人员遵循CobiT提供的“检查列表”来评估组织的合规性；

在机座机构，审计人员使用SP 800-53作为“检查列表”来评估机构的合规性。

它们有重叠也有差异，作为保护美国联邦系统的控制集，800-53描述了信息系统安全控制措施，为不同级别的系统推荐了不同强度的安全控制集(包括管理、技术和运行类)。为帮助机构对它们的信息系统选择合适的安全控制集，该指南提出了**基线**这一概念。基线安全控制是最小安全控制集，针对三类系统影响级别，它列出三套基线安全控制集(基本、中、高)。

②SP 800-53A Rev.1(联邦信息系统的安全访问控制指南，建立有效的安全评估计划)

是SP 800—53 Rev.3的附属指导方针，对信息系统的安全控制措施实施评估，它为创建有效的安全评估计划和联邦政府执行机构的信息系统中实施的程序进行安全控制措施有效性的评估提供指南。指南已经从技术层面发展到对国家安全系统的补充性指南，也可以在合适的联邦官员的允许下适用于国家安全系统。它用2个指标来评价程序实施，一个是深度depth，一个是广度coverage。

③SP 800-18 Rev.1(制定信息技术系统**安全计划指南**，2006年)（**第二域**）

为联邦机构对联邦信息系统制定系统安全计划提供了指南。描述了系统所有者、数据所有者、数据监管员等**角色**的职责。

5.配置管理类

①SP 800-128(信息系统安全配置管理指南，2010年)

为负责管理和执行联邦信息系统计算环境安全的机构提供指南，包括信息的处理、存储和通过外部或者面向服务的计算环境(如云计算环境提供者)进行传输的安全，指南的安全配置管理概念和原则可以帮助机构为外部计算服务的提供者建立保证的必要条件。

②SP 800-126 Rev.1(安全内容自动化协议技术规范(SCAP)，2010年)

定义了SCAP协议v1.1版本的技术规范，为系统配置的标准化以及对系统配置的脆弱性评估提供了一种统一的方法。

③SP 800-114(确保远程办公和远程访问外部设备用户指南)

帮助指导远程办公者使用的外部设备的安全，例如个人笔记本电脑以及手机等，文档特别关注于远程办公访问机构非公开计算资源的安全。

④SP 800-111(终端用户设备的存储加密技术指南)

帮助机构理解终端用户设备的存储加密技术，以及规划、实施和维护存储加密方案。

⑤SP 800-70 Rev.1(国内IT产品清单方案——用户和开发人员的指南)

方便开发和发布安全配置清单，帮助组织和个体用户更好地保护其信息技术产品，减少其被攻击的可能性。文档描述了安全配置列表和它们的优点，并解释了如何使用NCP查找和获取

列表，以及参与到 NCP 的策略、流程和通用要求。

⑥SP 800-27（信息技术安全工程原则-修订版 A）（**第三域**）

6.风险评估类

①SP 800-30(信息技术系统**风险管理指南**，2002 年)（**第一域**）

开发了一套风险管理方法：信息技术体系风险管理指南(Risk Management Guide for Information Technology System)。介绍了风险评估的步骤及方法，提供了一套用以开发出有效的风险管理过程的办法，以帮助组织更好地管理和 IT 相关的业务面临的风险。它包括对 IT 系统中风险评估和规避的定义和实践的指南，提供用于选择适当的安全控制措施的信息。

②SP 800-39(信息系统风险管理：组织的角度，2011 年)

是 NIST 开发的与 FISMA 相关的安全标准和指导方针系列中的旗舰文档，其中提供了一系列有意义的改进建议。文档旨在为集成的、组织范围的联邦信息系统的操作和使用来管理信息安全风险的程序提供指南，包括组织的运营(例如：任务、功能、形象和声望)、组织的评估等。

③SP 800-60 Rev.1(信息与信息系统安全分类的指南，2008 年)（**第二域**）

遵循 FISMA(电子政务法案的第三章联邦信息安全管理方案)的指导，为根据各种可能潜在的安全冲击对信息及信息系统进行分类提出指导方针，帮助联邦部门将不同的安全冲击级别映射到：(1)信息(如机密信息、医学信息、私人信息、金融信息、合约敏感信息、贸易机密信息、调查研究信息)；(2)信息系统(如任务评价系统、任务支持系统、行政管理系统)。此外，SP 800-53A 的安全控制措施评估也属于风险评估的一个步骤。

④SP 800-37 Rev.1（联邦信息系统风险管理框架 RMF：安全生命周期方法）（**第一域**）

为实施联邦信息系统的风险管理框架提供了指南，提出了将风险管理系统(RMF)应用于信息系统的方法。包括六步：安全分类、安全控制选择、安全控制实现、安全控制评估、信息系统授权和安全控制监管。即：

1)分类。对信息系统进行分类。

2)选择。选择该系统安全控制的初始化基线集，并根据风险和评估情况修订安全控制基线。

3)实施。实施安全控制，并描述如何部署控制。

4)评估。评估安全系统，确定一个范围以保证控制的有效实施并达到预期效果。

5)授权。允许信息系统可以正常运行和操作，确定其风险是可接受的。

6)监控。实时监控信息系统中的安全控制，掌握情况变化，分析并向特定组织机构报告系统的安全状态。

指出风险管理系统有以下特点：

1)鼓励其自动化操作，向高层领导者提供必要的辅助决策信息。

2)将信息安全与公司系统结构以及系统开发生命周期相结合。

3)强调选择、实施和评估以及安全控制的监管和信息系统的授权。

4)通过风险管理(功能)将系统层面与组织层面的风险管理过程相联系。

⑤SP 800-137（联邦信息系统和组织的信息安全持续监控 ISCM)（**第六域**）

安全实践者需要确定系统的监控频率或安全控制的评估频率时，把下列准则考虑在内：

1)安全控制的易变性：易变的安全控制应被更频繁地评估，无论评估目的在于确定安全控

制的有效性还是支持对度量指标的计算。

2)系统分类/影响水平：一般来说，分类为高影响度系统的安全控制要比中、低影响度的系统上被更频繁地监控。

3)提供关键功能的安全控制或特走评估目标：提供关键功能的安全控制或特定评估目标(比如日志管理服务器，防火墙)应当更频繁地被监控。另外，支持关键安全功能的个别评估目标被认为是对系统很关键的(根据业务影响分析)。

4)对于已经辨识的弱点的安全控制：一般认为，已经记录在安全评估报告(SARs)的现存风险需要更频繁地监控以确保风险在可容忍范围内。

5)组织风险容忍水平：对风险容忍水平低的组织(比如处理，存储，或传输大量专有和/或个人身份识别信息的组织，有大量高等级系统的组织，面临特定持续性威胁的组织〕会比对风险容忍水平高的组织(比如拥有大量中低等级的系统，基本不处理，存储或传输专有的/或个人身份识别信息的组织)更频繁地监控安全态势。

6)威胁信息：组织要考虑现有可信的威胁信息，包括已知的漏洞，攻击场景。

7)薄弱点信息：在决定监控频率时，组织要考虑与信息技术产品相关的最新薄弱点信息。比如,如果一个特定产品厂商每月提供软件补丁,组织就可以考虑至少每月一次执行漏洞扫描。

8)风险评估结果：检查组织的、或系统的风险评估结果，并在决定监控频率时考虑这些结果的影响。如果在组织内部有风险打分系统，风险的分值可能被用来证明增加或减少对相关控制的监控频率的合理性。

9)报告要求：报告要求不会驱动 ISCM 战略，但是可能对监控频率产生影响。比如如果组织策略要求每个季度报告非授权组件数量和采取的纠正性行动,组织将至少每季度监控系统以发现非授权组件。

二、ISO 27000 系列

对于企业组织来讲，就像个人要考 CISSP 认证一样，它也期望向获得认可的第三方机构寻求 ISO/IEC 27001 认证证书，可以证明其公司范围内的安全实践水平。还有什么 ISO-9001 认证的，都是为了证明资质、提高声誉。后面这些标准在 AIO6 书上都有详细描述，不会考具体内容的。

1.发展历程

英国标准 BS 7799(British Standard 7799)是由英国政府工贸部 1995 年开发并由英国标准化机构(British Standard Institution)发布。这个标准概括出信息安全管理体系 ISMS（又名安全规划）应该如何建立和维护。其目标是指导组织设计、实施和维护策略、过程及技术，以便于管理组织的敏感信息资产面临的风险。它包括 2 部分：第一部分，描述了控制目标和为实现这些目标可使用的控制措施范围（Code of Practice for Information Security Management），它于 2000 年被采纳为 ISO/IEC 17799，目前其最新版本为 2005 版，也就是常说的 ISO 17799：2005。；第二部分描述了如何建立和维护安全规划(for Information Security Managemenet Specification）(信息安全管理体系 ISMS)，同时也作为对组织进行认证的基线，其最新修订版在 2005 年正式成为 ISO-27001。

ISO 和 IEC 对 BS7799 进行了升级和优化，开发了 27000 系列标准，成为国际标准。它是

由信息安全方面的最佳惯例组成的一套全面的控制集，是信息安全管理方面最受推崇的国际标准。最重要的是 27001 和 27002。

①ISO-27000 基础原理与名词解释（Principles and vocabulary）

②**ISO-27001 信息安全管理体系-建设要求**（ISMS Requirements，以 BS 7799-2 为基础）

③**ISO-27002 信息安全管理体系-最佳实践**（以 ISO/IEC 17799：2005 为基础）

④ISO-27003 信息安全管理体系-实施指南

⑤**ISO-27004** 信息安全管理体系-测量指南与指标框架

⑥**ISO-27005** 信息安全管理体系-风险管理指南，规定在 ISMS 框架内如何进行风险管理

⑦ISO-27006 信息安全管理体系-审核与认证机构指南（Requirements for the accreditation of bodies providing certification）

1-5 记忆：要求、实践、实施、测量、风险管理。

2.ISO 其它的相关标准

①**ISO-15408** 1996 年六国七方签署了《信息技术安全评估通用准则》即 **CC** 1.0。1998 年美国、英国、加拿大、法国和德国共同签署了书面认可协议。后来这一标准称为 CC 标准，即 CC 2.0。CC 2.0 版于 1999 年成为国际标准 ISO/IEC 15408，我国于 2001 年直接来过来作为 GB/T 18336。 目前已经有 17 个国家签署了互认协议，即一个 IT 产品在英国通过 CC 评估以后，那么在美国就不需要再进行评估了，反之亦然。目前我国还未加入互认协议。

②ISO/IEC-**42010** 包含一套推荐做法，旨在简化软件密集型系统体系结构的设计和概念。这个标准提供了一种语言（术语）来描述软件体系结构和如何把它融入开发生命周期中。许多时候，开发人员实际开发时，不会完全参照某一个软件体系结构的整体标准，这个标准就提供了一个可遵循的概念框架。

③ISO/IEC-**27799** 医疗机构信息安全管理指南。

④ISO/IEC-21827：2008《系统安全工程能力成熟度模型》(SSE-CMM)（**第三域**）

该模型是安全工程实践规范的一种标准测量尺度，涵盖了以下方面：

1)整个生命周期，其中包括开发、操作、维护和退役方面的活动。

2)整个机构，其中包括机构层面和工程层面的活动。

3)与其他方面的交互，如系统、软件、硬件、人的因素、测试工程、系统管理、运维等。

4)与其他机构的交互，其中包括采购、系统管理、认证、认可和评估。

⑤ISO/IEC **27034**。关于软件开发的标准。ISO/IEC 27034 标准包括以下条目：应用安全综述和概念、组织规范框架、应用程序安全管理过程、应用安全验证以及特定应用的安全指南。它是 ISO/IEC 27000 系列的一部分，它能让安全的软件开发过程与 ISO/IEC 的信息安全管理体系(ISMS)模型相一致。

三、COBIT 目标/IT 治理

CobiT 信息及相关技术控制目标(Conrol Objectives for Information and related Technology)，是由国际信息系统审计协会(ISACA)和 IT 治理协会 ITGI 联合开发的 IT 管理控制目标集，记录了一整套优秀的 IT 安全实践，规定了对安全**控制的目标和要求**，鼓励将 IT 的理想安全目标映射到商业目标中，也可以作为组织审计的指导方针。对于 IT 治理，CobiT

提供了一个“检查列表”的方法，也就是在实现不同的 IT 功能时，需要提供一系列经过深思熟虑完成的材料。CobiT 规定了执行摘要、管理指南、框架、控制目标、实现工具集、性能指标、成功因素、成熟度模型和审计准则。它勾画出一个完整的可以遵循的路线图来完成这种模式涉及的 34 个控制目标中的每一个。CobiT 分成 4 个领域，每个领域又细分为子类别：

①计划和组织(Plan and Organize)

②获得与实现(Acquire and Implement)

③交付与支持(Deliver and Support)

④监控与评价(Monitor and Evaluate)

CobiT 规定了执行摘要、管理指南、框架、控制目标、实现工具集、性能指标、成功因素、成熟度模型和审计准则。它勾画出一个完整的可以遵循的路线图来完成这种模式涉及的 **34 个**控制目标中的每一个。COBIT 5 把驱动控制目标划分为七种动力因子，关于**企业 IT 治理**和管理的五个关键原则是：

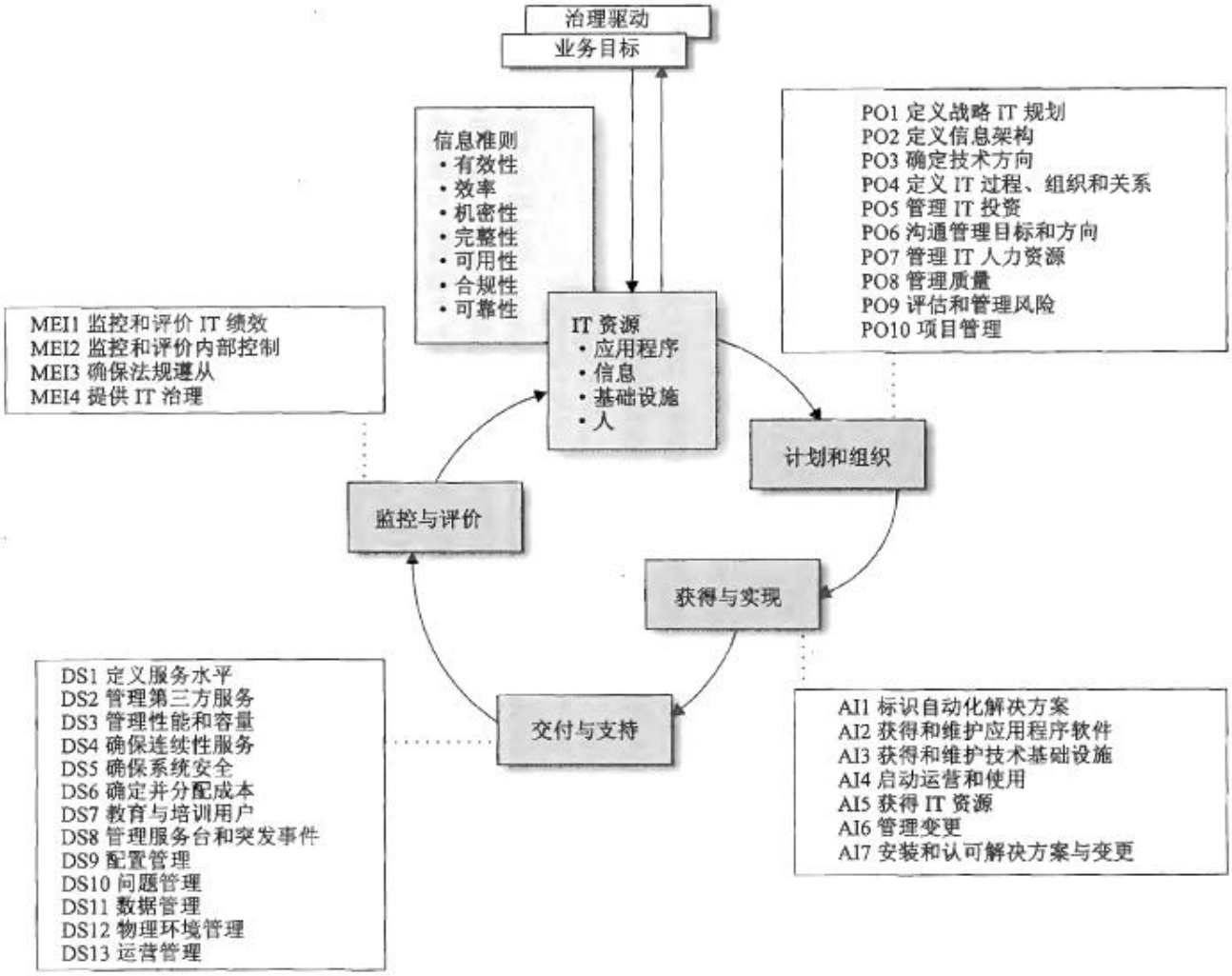
原则 1： 满足**利益**相关者的需求；Meeting stakeholder needs

原则 2： 对企业做到**端到端**的覆盖；Covering the enterprise end-to-end

原则 3： 使用**单一**的集成框架；applying a single integrated framework

原则 4： 使用**整合**处理法；enabling a holistic approach

原则 5： 把治理从管理中**分离**出来。Separating governance from management



四、ITIL 服务/流程管理

在当前市场环境下，客户服务的好坏直接受 IT 系统的影响，IT 服务管理成为企业业务运作过程中不可或缺的重要一环。需要强调的一点是：ITIL 不是一个正式标准，而是普遍实行的“事实”上的标准。

IT 基础架构库(Information Technology Infrastructure Library, ITIL)，即信息技术基础架构库,它是由英国商务部开发的用于 IT 服务管理的过程。由英国政府部门 CCTA(Central Computing and Telecommunications Agency)在 20 世纪 80 年代末制订，现由英国商务部 OGC(Office of Government Commerce)负责管理，主要用于 **IT 服务管理**（ITSM），提供了一个客观、严谨、可量化的标准和规范，也可用于其它领域。

1. ITIL 包含 6 个模块内容

业务管理、服务管理、ICT 基础架构管理、IT 服务管理规划与实施、应用管理和安全管理。其中服务管理是其最核心的模块，该模块包括“服务提供”和“服务支持”两个流程组。

2. ITIL 包含 5 个生命周期

①战略阶段（Service Strategy)；

②设计阶段（Service Design)；

③转换阶段（Service Transition)；

④运营阶段（Service Operation)；

⑤改进阶段（Service Improvement)。

3. ITIL 包括 5 类管理流程

①事件管理（Incident Management）

目标：在不影响业务的情况下，尽快恢复服务，以保证最佳的效率和服务的可持续性。

②问题管理（Problem Management）

目标：调查分析日志、事件等数据，确定事件隐患，提交服务中的潜在故障。

③配置管理（Configuration Management）

目标：定义和控制服务与基础设施的部件，并保持准确的配置信息。

④变更管理（Change Management）

目标：以受控的方式，确保所有变更得到评估、批准、实施和评审。

⑤发布管理（Release Management）

目标：在实际运行环境的发布中，交付、分发并跟踪一个或多个变更。

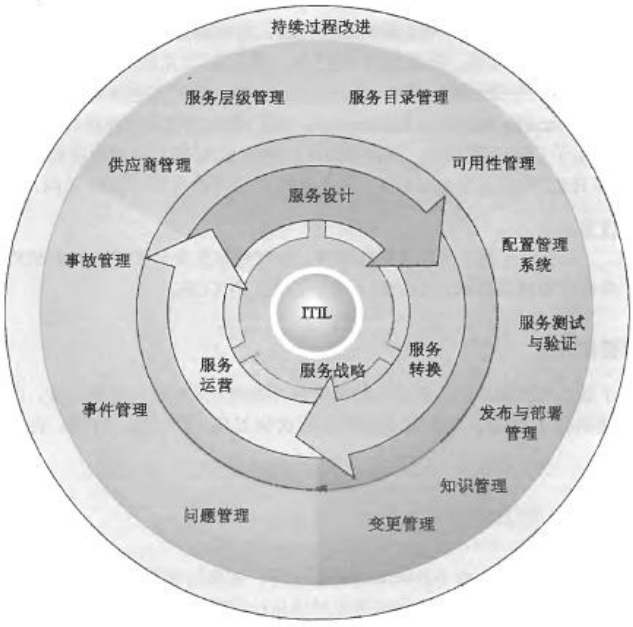


图 2-8 ITIL

五、COSO/企业内控

其实 CobiT 是从 COSO 演变而来的。但 COSO 是**企业**治理模型，而 CobiT 是 **IT** 治理模型。

COSO 委员会是专门研究内部控制问题的。COSO 就是美国反虚假财务报告委员会下属的发起人委员会的英文缩写（The Committee of Sponsoring Organizations of the Treadway Commission）。1992，COSO 委员会发布《内部控制整合框架》，简称 COSO 报告，1994 年进行了增补。根据 2002 年萨班斯法案第 404 节条款（SOX）以及美国证券交易委员会（SEC）的相应实施标准，要求：公众公司的管理层评估和报告公司最近年度的财务报告的内部控制的有效性。这表明 COSO 框架已正式成为美国上市公司内部控制框架的参照性标准。COSO 报告提出内部控制是用以促进效率，减少资产损失风险，帮助保证财务报告的可靠性和对法律法规的遵从。总之，COSO 用于**公司内部治理**，由反欺诈财务报告全国委员会发起组织委员会(COSO)开发，旨在帮助降低财务欺诈风险的国内公司**控制集**。COSO-2013 标准有 4 个目标和 8 个组成部分。

1.COSO 内部控制的 4 个目标

①符合企业的长期目标；

②经营高效、用好资源、卓有成效；

③可靠的财务报告；

④合规。

2.COSO 的 8 个组成部分

①内部环境：考虑风险基准（基线）

②设定目标：管理过程来支持和配合企业的目标

③事件识别：确定内部和外部影响企业目标的事件。

④风险评估：考虑可能性和影响，以及怎样管理这些风险属性。

⑤风险响应：对每个资产，选择一种适当的应对措施：接受、减缓、转移或回避（拒绝）。

⑥控制活动：制定并执行策略，确保风险响应的有效性。

⑦信息和沟通：获取并共享相关信息，使人员能够履行他们的职责。

⑧监控：评估整个 ERM（企业风险管理）活动，并做出必要的改变。

C.2 安全与风险管理方面

1.安全方案开发

ISO/IEC 27000 系列

2.企业架构开发

①Zachman：全球第一个企业架构开发模型，是一种逻辑结构，用一种可以理解的信息来表述企业架构。该框架采用了一种 6 行,每行中包含 36 个子单元的格式：

六行包括了——范围、商业模式、系统模式、技术模式、组件、工作系统；

六列分别为——谁、什么、什么时间、什么地点、为什么、如何做。

②TOGAF：开放组体系结构框架(The Open Group Architecture Framework)是行业标准的体系架构框架，可以被任务组织自由使用。它由国际标准权威组织 The Open Group 制定。

③DODAF：美国国防部制定的系统体系结构框架，其前身是 C4ISR，用于保障军事任务完成过程中系统间的互操作性，提供了 8 种不同角度的视图。

④MODAF：英国国防部体系架构框架（MODAF）也是一个架构框架，最初的目的是支持网络使能能力（NEC）。

3.安全架构开发

SABSA 安全架构框架(Sherwood Applied Business Security Architecture)：

SABSA®是一个方法论，它通过开发以风险作为驱动的企业信息安全和企业信息保证结构来派生以支持关键商务的安全架构解决方案。它是一个开放式的标准，包括了大量的框架、模型、方法和步骤，是完全免费。SABSA 也是独一无二的、完全中立的、可伸缩的，也其他标准无缝结合，如 TOGAF 和 ITIL 什么的，并填补了“安全架构”和“安全服务管理”之间的空隙。

它是一个开发安全架构的完整生命周期，第一步是评估业务需求。它生成一个“追溯链”chain of traceability，用来描述各业务功能的安全需求，还包括策略、概念、设计、实现和度量等阶段。它用 6 层结构来表示任何架构，每层代表一个不同的视角，比如的设计、施工和使用目标系统等。

4.公司治理

COSO 企业内控管理模型。

5.安全控制开发

①COBIT IT 内部控制；

②NIST 800-53 安全控制参考（基线）。

6.流程管理

①CMMI 能力成熟度模型集成(Capability Maturity Model Integration)：模型由卡内基·梅隆大学开发，目的是优化组织的开发过程，如标准化的软件开发管理；

②ITIL 服务管理；

③六西格玛 Six Sigma：是一种过程改进方法论，也是一种业务流程管理的管理策略，摩托罗拉工程师搞的，是一种改善企业质量流程管理的技术，以“零缺陷”的完美商业追求，带动质量成本的大幅度降低，最终实现财务成效的提升与企业竞争力的突破，是用来开展过程改进的业务管理策略。其目标是在生产过程中识别和消除缺陷。六西格玛背后的原理就是如果你

检测到你的项目中有多少缺陷，你就可以找出一一应对的办法，使你的项目尽量完美的方法。它是 TQM 的升级。企业要想达到六西格玛标准，它的出错率不能超过百万分之 3.4。

7.其他

①PMBOK, Prince2 项目管理；②ISO9000 质量管理；③ISO 38500 IT 治理；④ISO22301 业务连续性管理。

8.风险评估的模型

①**FRAP**(Facilitated Risk Analysis Process)：专用的定量方法，先进行预筛选以节省时间和金钱。

②**OCTAVE**(Operationally Critical Tbreat, Asset and Vulnerability Evaluation)：面向团队的方法，通过组织研讨会来评估组织风险和 IT 风险。

③**AS/NZS 4360**：澳大利亚和新西兰的一种业务风险管理评估方法。

④**失效模式和影响分析 FMEA**(Failure Modes and Effect Analysis)：美国航天 NASA 搞的，是一种用来确定潜在失效模式及其原因的分析方法，可在产品设计或生产工艺真正实现之前发现产品的弱点，可在原形样机阶段或在大批量生产之前确定产品缺陷。FMEA 有三种类型：分别是系统 FMEA、设计 FMEA 和工艺 FMEA。

⑤**故障树分析 Fault Tree Analysis/FTA**：美国贝尔公司搞的，是安全系统工程中最重要的分析方法。事故树分析从一个可能的事故开始，自上而下、一层层的寻找顶事件的直接原因和间接原因事件，直到基本原因事件，并用逻辑图把这些事件之间的逻辑关系表达出来。特点是直观明了，思路清晰，逻辑性强，可以做定性分析，也可以做定量分析。

⑥**CRAMM** 中央计算和电信机构风险分析管理方法：Central Computing and Telecommunications Agency Risk Analysis and Management Method。

C.3 计算机犯罪方面

1.计算机诈骗和滥用法案（Computer Fraud and Abuse Act）（历史第一个）

国会在 1984 年制定了计算机诈骗和滥用法案（CFAA），主要针对下列罪行：

①非法访问联邦系统中的机密信息或财务信息。

②非法访问联邦政府使用的计算机，以及联邦计算机进行欺诈活动

③对联邦计算机系统造成恶意损失超过 5000 美元的行为。

④非法修改计算机中的医疗记录。

⑤非法买卖计算机密码。

该法案在 1986 年进行了修正，主要拓展了使用范围，涵盖了：

①由美国政府专门使用的所有计算机。

②由金融机构专门使用的所有计算机。

③被用于进行犯罪的所有计算机组合。

2.计算机安全法案（CSA 1987 年）Computer Security Act of 1987

国会还是不满 CFAA 的 1986 修正案，又制定了计算机安全法案(1987 年)，为所有的联邦机构设置了安全要求基准。CSA 的四个主要目的是：

①明确由美国国家标准技术研究所(NIST)负责开发联邦计算机系统标准和准则，由美国国

家安全局(NSA)提供技术性建议和援助。

②颁布并施行上述的标准和准则。

③要求所有使用涉密联邦计算机系统的操作人员，都要制定安全计划。

④所有相关的 管理、使用和操作人员强制性参加定期培训。

⑤它还指定了 NIST 负责公开系统的安防，NSA 负责机密级系统的安防。

这条法案的相关要求经过多年演进后，形成了联邦计算机安全策略的基础。

3. CFAA 修正案（1994 年）

1994 年，国会对上述法案又进行了大改。包括以下条款：

①生成任何类型恶意代码的行为是不合法的。

②法案适用于所有被用于州间贸易的计算机。

③允许关押罪犯，不管他们是否造成了实际的损坏。

④计算机犯罪的受害者可以提起民事诉讼，其受到的损失可以获得减轻和补偿。

2015 年，奥巴马也准备做个修改，把计算机犯罪纳入 RICO 条款范围中，即反诈骗腐败组织集团犯罪法(the Racketeer Influenced and Corrupt Organizations Act)，不知道现在正式颁布没有。

4.国家信息基础设施保护法案(1996 年)（National Information Infrastructure Protection Act of 1996）

1996 年，国会还是不满 CFAA，又通过了一系列修正案，再进一步扩展了其保护的范围，包括以下新覆盖的领域：

①放宽了法案的范围，除了用于州间贸易的计算机，还包括用于国际贸易的计算机系统。

②扩展了对国家基础设施(铁路、燃气、电力和通信线路等)的类似保护。

③故意造成国家基础设施重大损坏的行为，要从重处理。

5.联邦判决指导方针（Federal Sentencing Guidelines）

1991 年发布的联邦判决指导方针主要提供计算机犯罪的处罚指导、解释说明等，它最重要的三个条款是：

①提出**审慎者规则**（prudent man rule）。就是要谨慎工作，这种规则要求高管确保他能常态化的、持续的保持适度关注（due care）的态度；其它人员同样也要求保持谨慎工作的态度。这个规则以前用在在财政领域。（就是领导责任制）

②提出从轻处罚规则。对于有违法行为的组织机构和执行官，如果它能证明其保持并运用了适度关注的原则，并履行了自己的信息安全责任，那么可以从轻处罚。

③明确了要证明疏忽或差错确实成立的三个要素。即：被控人员必须具有法律上认可的责任；被控人员必须未遵守公认的标准；疏忽行为和后续损害之间必须存在因果关系。

④高管渎职可以处以最高 2 亿美元的罚款。

6.文书精简法案(1995 年)（Paperwork Reduction Act of 1995）

文书精简法案（199 年）要求组织机构必须获得美国行政管理和预算局 OMB(Office of Management and Budget) 的批准后，才能请求使用各类基础公共信息。2000 年的政府信息安全改革法案 GISRA（The Government Information Security Reform Act）对它进行了修正。

7.政府信息安全改革法案(2000 年) GISRA （Government Information Security Reform

Act of 2000）

国会要求 GISRA-2000 的拟制满足以下**五个基本目标：**

①要提供 1 个内容全面的体制。确保所有政府相关的信息资源安全、有效。

②要确保网络协同安全、有效。一切系统都是基于网络的，所以必须安全。

③要有效监控和掌握所有与安全风险相关的活动和信息。每个人的每个行为都要被监控。

④开发和维护联邦政府的信息安全防护系统。既要满足安全需求，也要实现最小成本。

⑤提供改进机制。能持续优化、完善联邦机构的信息安全监督体系。

GISRA 仍然明确，NIST 负责非机密系统，NSA 负责机密系统，并实行领导负责制。

GISRA 重新定义了计算机系统的分类，明确了**关键系统要满足以下条件：**

①被法律条款定义为国家安全系统。

②有机密信息且被相应的措施保护。

③系统被攻击会对机构的业务产生不良影响。

在这之后，国会总算不再折腾了，没有通过任何新的关于计算机犯罪的重大事项。虽然提了一些草案，都还没通过，如：2012 年的网络安全法案和 2013 年的网络情报共享和保护法案。

8.联邦信息安全管理法案 FISMA（Federal Information Security Management Act）

在 2002 年通过的联邦信息安全管理法案（FISMA），要求联邦政府实施一个信息安全项目，涵盖了政府部门的运营和外包商的活动。NIST 开发了 FISMA 的实施指南，提出了确保信息安全项目有效的关键要素：定期评估风险、安全意识培训、定期渗透测试、记录突发情况、制定应急响应流程等。

C.4 保护知识产权方面

1.数字千禧年版权法案(DMCA)（Digital Millennium Copyright Act）

DMCA 中有 2 个条款（**打击盗版**）：

①阻止用户破坏版权保护机制。非法的复制会被处以巨额罚款。

②网络服务商（ISP）的线路被用于传播盗版，也要承担相应的责任。

2.经济间谍法案(1996 年)(Economic Espionage Act of 1996)

经济间谍法案（1996 年）主要有 2 个规定：

①任何被发现为外国政府或机构而从美国公司窃取商业秘密的人，可以被处以高达 50 万美元的罚款和长达 15 年的监禁。

②任何被发现其它情况中窃取商业秘密的人，可以处以 25 万美元的罚款和 10 年的监禁。

3.统一计算机信息处理法案 UCITA（Uniform Computer Information Transactions Act）

统一计算机信息处理法案(UCITA)，提供了计算机相关业务处理的共同架构，包括对**软件许可证** software license 颁发的规定。UCITA 为各种形式的许可提供了法律描述和保护。还要求用户可以在安装之前拒绝许可证协议，生产商必须全额退款。它要求不同州之间的“许可协议”都符合统一的标准。

4.瓦森纳协议(Wassenaar Arrangement)

WA 是对“常规武器和两用货品及技术”实施进出口管制的法律，来用阻止恐怖国家的军事实力增强，由 40 个国家共同制定了 9 类端口的出口规范，包括特殊材料、高科技设备、保

密机等产品。

C.4 个人隐私方面

一、美国有关隐私的法律

好多，眼花缭乱。

①第四修正案（Fourth Amendment of the Constitution）

隐私权的基础是美国宪法的第四修正案，内容如下：法律保护个人的人身、房屋、证件和财物不受无理的搜查和没收。搜查检索必须要有许可。

②隐私法案(1974 年)（Federal Privacy Act of 1974）

美国的隐私法案(1974 年)是对美国联邦政府有关公民个人私有信息处理的最重要的法律。任何机构在没有得到当事人书面同意的情况下，不得向他人泄漏隐私信息。

③电子通信隐私法案(1986 年)ECPA（Electronic Communications Privacy Act of 1986）

电子通信隐私法案(ECPA)规定对个人电子隐私的侵犯是犯罪行为。最重要的规定禁止窃听，否则处以最高达 500 美元的罚款和最高 5 年的监禁。（其实美国在窃听全世界）

④执法通信协助法案(1994 年)CALEA（Communications Assistance for Law Enforcement Act）

执法通信协助法案(CALEA)是对上面那个 1986 年的电子通信隐私法案的修正。它要求通信运营商允许持有法院命令的执法人员进行合法窃听。

⑤经济和专有信息保护法案(1996 年)EPPA（Economic and Protection of Proprietary information Act of 1996）

该法案将经济信息也视为财产，盗窃并不局限于物理产品。

⑥健康保险的流通和责任法案(1996 年)HIPAA（Health Insurance Portability and Accountability Act of 1996）

HIPPA 经常被考到，它要求医院、医师、保险公司和其它处理或存储个人医疗隐私信息的组织采取严格的安全措施，明确定义了个人在医疗记录方面的权利。

⑦2009 关于经济和临床健康的卫生信息技术法案 HITECH（Health Information Technology for Economic and Clinical Health Act of 2009）

关于经济和临床健康的卫生信息技术法案(HITECH)对 HIPAA 进行了修订。主要变化是针对商业伙伴(BAs)的。它将所有相关机构定义为：处理被保护的健康信息（PHI）的组织机构。任何 PHI 机构和一个商业伙伴（BA）之间的关系必须有书面合同管理，这个合同被称为业务联合协议（business associate agreement，BAA）。

HITECH 是全国性的法律。此外，每个州都颁布了自己的相关法规。加利福尼亚州的 SB1386 是第一个发布的，涉及以下隐私信息：社会保险号、驾照号码、身份证号码、信用卡或借记卡号码、银行账户与安全代码、病历、医疗保险信息等。

HITECH 还明确了数据泄露的通告范围：发生泄密事件的 PHI 机构必须通知受影响的个人，影响超过 500 人时，必须通知卫生和人事服务部（the Secretary of Health and Human Services）的部长和媒体。

⑧数据泄露通知法 DBNL（Data Breach Notification Laws）

若有泄密事件，当事单位必须在 60 天以内通知个人信息被非法访问。（如果影响超过 500 个人，还必须向媒体发布相关事件）。

⑨儿童联机隐私保护法案(1998 年)COPPA（Children’s Online Privacy Protection Act of 1998）

儿童联机隐私保护法案（COPPA）对儿童网站的信息保护提出了一系列要求。它要求任务组织必须要取得父母的同意后，才能收集 13 岁以下儿童的信息。

⑩Gramm-leach-Bliley 法案(1999 年) GLBA/金融服务现代化法案/格蕾姆

GLBA-1999，严格限制了银行、保险公司等商业机构之间的信息共享和服务提供，还要机构定期向用户发对账单。

⑪美国爱国者法案(2001 年)（USA PATRIOT Act of 2001）

这个是国会对 2001 年 911 事件的响应。它扩大情报机构的权限，将以前一次只能获取一条线路的监听授权扩大为可以获得对一个人的有所通信进行监听的一揽子授权。另一方面，允许网络服务提供商(ISPs)提供更多的信息。它还修正了计算机欺诈和滥用法案（CFAA），对犯罪行为从重处理。

⑫子女教育权利和隐私法案 FERPA（Family Educational Rights and Privacy Act）

FERPA 是关于教育机构的，保护成年学生和未成年学生父母的隐私权。

⑬身份偷窃和冒用阻止法案(1998 年)（Identity and Assumption Deterrence Act）

就是规定身份偷窃是严重的犯罪行为。

⑭萨班斯-奥克斯利法案(SOX-2002) Sarbanes-Oxley ACT

2002 年的该法案(简称为 SOX)适用于在美国上市的任何公司，其中的许多法律被用于监管会计行为以及公司上报财务状况所使用的方法。然而，某些部分(特别是 404 条款)直接适用于信息技术。SOX 对公司如何追踪、管理和报告财务信息提出了专门要求，这包括保护财务数据并保证它的完整性与真实性。大多数公司都依赖计算机设备和电子存储来进行事务处理和数据归档，因此公司必须采用适当的流程和控制来保护这些数据。公司管理人员，包括首席执行官(CEO)、首席财务官(CFO)和其他人员，如果不遵守 Sarbanes-Oxley 法案，那么可能导致严厉的处罚，甚至可能会入狱数年。

二、欧盟有关隐私的法律

①概括指令/数据保护指令（directive outlining privacy measures）《指令 95/46/EC》

1995 年，欧盟(EU)议会也通过了描述隐私措施的概括指令（directive outlining privacy measures）。要求所有个人数据的处理要满足有关标准，明确了个人对自己信息的处理权利。

②美国—欧盟安全港湾项目/安全避难所（避风港 Safe Harbor program）

经过与联邦数据保护和信息、委员会的商讨，美国商务部开发了独立的安全港湾框架来调和欧美对于隐私不同的处理方式，并给美国组织提供一种优化的方法以符合欧盟数据保护法的要求：数据出口方和进口方之间的合同必须需要事先获得国家数据保护当局的批准，方可传输数据到国外。为了符合安全避难所规定，在欧洲进行商业活动的美国公司必须满足 7 项处理个人信息的要求。这里强调下经常考的 7 个安全港原则。这是美国贸易部的一个控制机制，防止未授权的信息泄露，相关的术语有：

1)通知 notice：任何组织必须告知个人使用数据的目的。（告知我）

2)选择 Choice：任何组织必须为个人提供可选择的机会。（我选择）

3)向前传输 Onward transfer：组织只有在遵守通知及选择规则的基础上才能向其他组织传输资料。（别乱传）

4)安全 Security：组织必须保护好数据。（别泄密）

5)数据完整 Data integrity：组织不得将信息挪用，还要确保数据真实可信。（别乱改）

6)访问 Access：个人可以查、改或删组织所持有的他们的个人信息。（属于我）

7)执行 Enforcement：组织必须落实以上各条原则。（别搞事）

三、支付卡行业数据安全标准（Payment Card Industry Data Security Standard）

支付卡行业数据安全标准(PCI-DSS) 是一个非法律但有合同义务的优秀合规要求典范。有 12 个主要要求，不列举了。它提供了一系列关于支付安全控制的标准。

四、数据泄露方面的

1.电子通信服务规范(Regulation for Electronic Communication Service, EU: 2013)

欧洲电子通信服务提供者，需要在检测到个人数据泄露后不迟于 24 小时向国家主管当局提供个人数据泄露的数据泄露通知。

2.隐私和电子通信法规(Privacy and Electronic Communications Regulations.UK: 2013)

电子通信服务提供商，诸如电信，互联网服务供应商(ISPs)，在知道数据泄露的基本事实后必须在 24 小时内通知 UK 信息专员办公室。

C.5 业务连续性方面

1.NIST 800-34 中的业务连续性规划的流程

业务连续性规划中的业务影响分析 BIA 是很重要的内容，在第一域的 G.2 章节已经详述了相关流程。

NIST800-34 文档是专门针对 IT 的应急计划，当然，它也同样适用于制定企业级的 BCP 和 BCM。所有的团队成员都有义务参加变更控制程序。评审应按 BCP/DRP 策略进行，一般每 3 个月组织 1 次审查，每年进行 1 次正式审核，或者有任何重大的组织改变的时候。

①制定业务连续性规划策略声明。——连续性策略，为计划和建立 BCP 的工作提供了框架和管理，包括：范围、任务、原则、指南和标准。

②进行业务影响分析（BIA）。——业务影响分析，包括风险评估和资产赋值，流程为：搞数据收集、定关键业务、定依赖资源、算资源寿命、定漏洞威胁、算业务风险、写分析报告。

③制定预防性控制方法。——控制措施

④制定恢复战略。——恢复战略

⑤制订应急计划。——制定 BCP

⑥测试计划及进行培训和演练。——测试和演练

⑦维护计划。——维护计划

项目的单个目标必须进行分析，证明计划是有用可行的，确保每一个目标是能够实现的。即 **SWOT 分析**，其基本元素包括：

*优势 Strengths——项目团队的特点，使其比其他团队具有更大的优势。

*劣势 Weaknesses——相对于其他团队，使该团队处于不利地位的特征。

*机会 Opportunities——可以促进项目成功的元素。

*威胁 Threats——可能促使项目失败的元素。

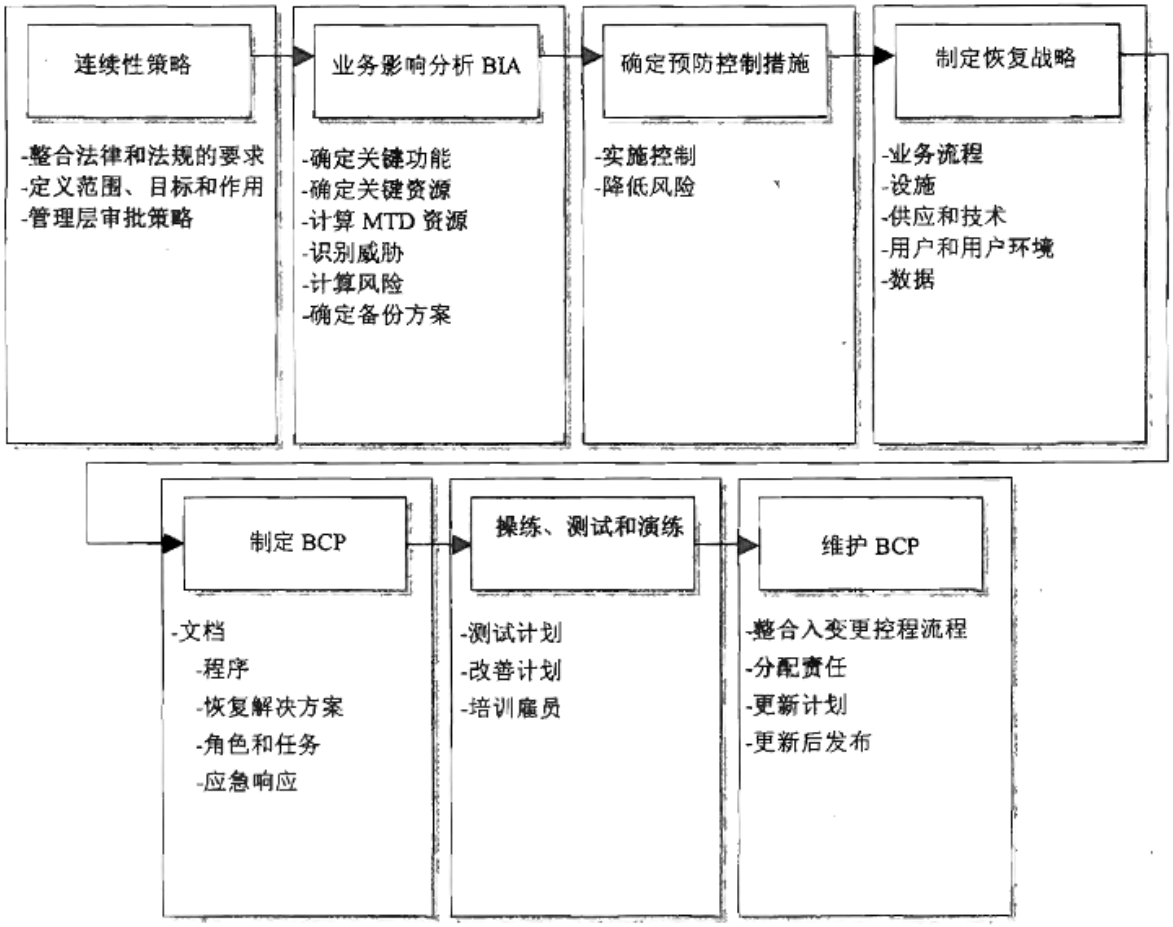


图 8-4　制定业务连续性规划的步骤

①**BS 25999**

英国标准协会(BSI)的业务连续性管理(BCM)标准。BS 标准有两个部分：

*25999-1：2006 BCM 业务守则，提供过程、原则、术语体系，即提供业务连续性管理的相应过程、原则和术语体系的一般指南。

*25999-2：2006 BCM 规范，说明执行目标及审核需求，即细说明执行、运作和增强一个 BCM 系统的目标以及审核需求。

②**ISO/IEC27031：2011 业务连续性的 ICT(信息和通信技术)准备指南。**

此标准是 ISO/IEC27000 整个系列标准的一个组成部分。

③**ISO 22301**

业务连续性管理体系的国际标准，取代 BS-25999-2。

④**GPG（业务连续性协会的优秀实践指南）**

BCM 的最佳实践，分为管理实践和技术实践：
*管理实践方面：策略和程序管理；在组织文化中嵌入 BCM。
*技术实践方面：理解组织；确定 BCM 战略；制定和实施 BCM 响应；演练、维护和修订。
⑤DRI 国际协议的业务连续性规划人员专业实践
将业务连续性管理流程分解为以下 10 个部分：
*项目启动和管理。　*风险评估和控制。
*业务影响分析。　*业务连续性战略
*应急响应和运作。　*业务连续性规划
*宣传和培训计划。　*业务持续计划演练、审核和维护
*危机沟通。　*与外部代理机构的协调

ISO/IEC270031：2011
业务连续性的 ICT（信息和通信技术）准备指南。

BS-25999
业务连续性管理标准（BCM），包括：
25999-1：2006 BCM 业务守则，提供过程、原则、术语体系。
25999-2：2006 BCM 规范，说明执行目标及审核需求。

ISO22301
业务连续性管理体系的国际标准，面向准备进行认证的组织机构，取代 BS-25999-2

NIST800-34
概述了信息技术系统的业务连续性指南（即针对 IT 的应急计划）
①制定业务连续性规划策略声明。
②进行业务影响分析（BIA）。
③制定预防性控制方法。
④制定恢复战略。
⑤制订应急计划。
⑥测试计划及进行培训和演练。
⑦维护计划。

GPG（业务连续性协议的优秀实践指南）
BCM 的最佳实践，分为管理实践和技术实践：

DRI 国际协议的业务连续性规划人员专业实践
将业务连续性管理流程分解为以下几个部分：

C.6 法律法规方面

欧洲理事会网络犯罪公约(Council of Europe (CoE) Convention on Cybercrime)

是针对网络犯罪而尝试创建的一个国际性标准。它是第一个通过协调国际法和改善调查技术与国际合作来打击计算机犯罪的国际公约。这个公约的目标包括形成一个框架，用于建立被告的司法裁判和引渡。例如，只有双方都裁判具体事件是犯罪时，才可能进行引渡。

经济合作与发展组织((Organisation for Economic Co-operation and Development, DECD)指导原则以及越境信息流(transborder informationflow)规则。

DECD 为不同的国家提供交换数据的指导原则，以对数据进行适当保护，帮助不同的政府展开合作，处理全球化经济所面临的经济、社会和管理挑战。

欧洲的数据保护目录((Data Protection Directive)和欧盟隐私原则(European Union Principles on Privacy)

欧盟原则主要与使用和传输敏感数据有关，它被包含在欧洲的数据保护目录((Data Protection Directive)中。任何想要与欧盟国家做生意的企业如果涉及敏感数据交换，需要遵照这些原则和数据保护目录。欧盟的隐私保障比其它国家要严格很多。

SAS70

审计员用来评估服务机构的控制措施的一套审计标准，它涉及顾客对财务报告的内部控制。计算机业延伸了 SAS70 的用途，还有其他类型的评估方法，如 WebTrust(电子商务控制)和 SysTrust(营控制)，但上述这 3 种评估标准都不能满足从整体上确保外包服务安全可靠的需要。所以又开发了新的评估标准来更好地满足公司的需要。那就是：

服务组织控制(Service Organization Controls, SOC)

SOC 1：关于金融控制。

SOC 2：关于信托服务(安全性、可用性、机密性、处理完整性和保密性)。

SOC 3：关于信托服务(安全性、可用性、机密性、处理完整性和保密性)。

SOC2 和 SOC3 的区别：

SOC 2 报告是关于信托服务的公司所采取的控制措施的详细数据，描述了审计员所做的测试、测试结果和审计员对每个控制措施和系统有效性的意见，并不提供给公众。

SOC 3 报告只陈述系统是否符合特定信托服务的标准要求，没有测试信息和控制措施的详细信息，可以用于通用目的，通常被用作“认可标识”，放置在服务提供商的网站和营销担保物上。

ISO/IEC27002：2005

其中 6.2.1 条款提到的“识别外部单位相关的风险”，用于在聘请第三方服务供应商之前，对信息安全问题应加以界定和评估。

PCI-DSS 标准

GPC 计划（治理、风险和合规计划）

业务记录特例/例外规则或业务进入规则

美国联邦证据法规（Federal Rules of Evidence FRE）的传闻规则中的一个法律特例，它表明，下列情况中的任何记录是被承认的：①记录是在正常的业务过程中作出的；②该业务定期作出这样的记录；③是在或者接近被记录事件发生的时间做出的；④该记录包含由知悉该文档内信息的人传输的信息。

E. 攻击方法汇总

考试所有相关的攻击进行归纳、合并、罗列，教材中同一攻击会在多个章节中反复出现。

一、破坏机密性的攻击（第一域）

捕获网络通信、窃取密码、文件、社会工程、端口扫描、肩窥、偷听和嗅探攻击等。

造成机密性遭到破坏的非恶意攻击的意外事件有：未对传输数据进行加密，在传输数据之前，未对远程系统进行充分的身份认证，一直打开不安全的接入点，访问恶意代码导致打开后门，甚至在显示器上显示数据的时候，人从访问终端离开等。

二、破坏完整性的攻击（第一域）

病毒、逻辑炸弹、未授权访问、编码和应用程序的错误、恶意修改、有企图的替换以及系统后门。造成完整性破坏的非恶意攻击的意外事件有：意外地删除文件，输入无效数据，更改配置，命令、代码和脚本中包含错误，引入病毒以及执行恶意代码(例如特洛伊木马)等。

三、破坏可用性的攻击（第一域）

对可用性的威胁或攻击有很多，包括：设备故障、软件错误、环境问题(如高温、静电、洪水、断电等)，还包括 DoS 攻击、客体损坏和通信中断等。造成完整性破坏的非恶意攻击的意外事件有：意外地删除文件，硬件或软件组件的使用过度，私下分配资源，贴错标签或不正确的客体分类。

四、基于客户端的攻击（第三域）

主要是本地缓存攻击

①ARP 缓存中毒

ARP 协议是将 IP 地址解析为 MAC 地址的协议。这种攻击使客户端传输的数据流发送给不是预期的其它系统（另一个 MAC 地址），这种攻击也被用来做中间人攻击。动态 ARP 缓存：攻击者回应 ARP 广播查询并发送伪造的回复，这样 ARP 缓存一起缓存，直到超时（通常是 10 分钟）。静态 ARP 缓存：本地执行 ARP 命令，这需要通过木马、缓冲区溢出或社会工程攻击才能在客户端运行。

②DNS 缓存中毒

另一个比较流行的中间人攻击方式，类似于 ARP 缓存，让主机访问别的地址。主要手段有：主机中毒、授权 DNS 服务器攻击、缓存 DNS 服务器攻击、DNS 查找地址改变以及 DNS 查询欺骗。

主机文件 HOSTS file：将常用的或访问过的域名（域名也被称为 FQDN：fully qualified domain name）与 IP 地址的映射存储在本地，方便下次上网用，提高速度。修改这个文件就可以让访问重新定向。

授权 DNS 服务器攻击 Authorized DNS server：直接修改权威 DNS 服务器（根服务器）的数据库，于是全网的域名解析都被篡改了，很严重，所以很快会被发现并纠正的。

缓存 DNS 服务器攻击 caching DNS servers：运营商或企业为了速度，缓存了从其他 DNS 服务器获得的 DNS 信息，搞它要容易多了，也不易被发现。

DNS 查找地址改变 DNS lookup address changing：这个很直接，通过修改 DHCP 服务器或修改本地静态 IP 地址，篡改主机的 DNS 地址，让主机到另一个伪造的 DNS 服务器上去查询。

DNS 查询欺骗 DNS query spoofing：这个有点难，但也经常发生。攻击者截获主机的 DNS 查询请求，然后发回错误的结果，让主机访问错误的网站，把 DNS 服务器屏蔽了。

③Internet 临时文件中毒

上网浏览时，所有网站的内容都被缓存到本地的临时文件夹里。被植马的网站页面文件（图片、HTML 什么的）会被缓存到本地，然后就等待被调用或激活。

五、针对密码加密的攻击（第三域）

①分析攻击（Analytic Attack）/代数攻击。分析并利用算法本身的数学逻辑性，找出更简单的替代的算法。

②实现攻击（Implementation Attack）/执行攻击。利用加密程序存在的漏洞，简单易行，破密**首选**。包括 3 种形式：

*旁路攻击 Side-channel analysis，依靠能量消耗、放射性等密码系统运行时的物理属性来攻击，如计时分析和电磁差分分析。

*故障分析 Fault Analysis，通过注入错误信息来对比、记录、分析系统的加密漏洞。

*探测攻击 Probing Attacks，在密码模块周边进行探测和注入，希望能采集到算法或密钥什么的。

③统计攻击（Statistical Attack）。利用密码系统的统计弱点，例如无法真正生成随机数，浮点运算的错误等。统计攻击试图发现运行密码系统的硬件或操作系统的漏洞。

④穷举攻击（Brute Force/Exhaustive search）。暴力攻击。为了提高速度，通常使用彩虹表。密码一般以散列值的方式存在数据库里，彩虹表是预先计算和整理出的散列值映射表，可以大幅提高猜解速度。

⑤仅知密文/唯密文攻击（Ciphertext Only Attack）。最难的攻击，因为只有几条密文，其它啥也没有。只能通过频率分析进行统计学的攻击和预测。因为 26 个字母中，E,T,O,A,I,是出现频率最高的。

⑥已知明文攻击（Known Plaintext）。手上有明文，也有密文，然后想办法破解。

⑦选定密文/可选密文攻击（Chosen Ciphertext）。手上有密文，只有部分密文有明文。

⑧选定明文/可选明文攻击（Chosen Plaintext）。可以加密部分明文得到密文。

⑨中间相遇攻击（Meet in the Middle）。面向加密运算，通过计算查找出密钥对（K1加密的密文可以用K2解密），便两轮加密算法即双重DES(2DES)的实际强度和一轮加密一样。

⑩中间人攻击（Man in the Middle）。面向通信链路，在攻击者以通信代理的方式插入收发又方的通信，截获所有数据流。

⑪生日攻击（Birthday）。也称为冲突攻击或逆向散列匹配，利用生日悖论来进行穷举攻击和字典攻击，寻找可以生成相同消息摘要的不同消息。

⑫重放攻击（Replay）。既然破不了密，就截获加密的消息，下次直接重复使用它来进行身份验证什么的。如果系统有时间戳，这个方法就不能用了。

⑬微分/差分密码分析(differential cryptanalysis)。

差分密码分析攻击以找出加密密钥为目标。这种攻击会查看对具有特定差异的明文进行加密而生成的密文对，并且分析这些差异的影响和结果。它在1990 年作为一种针对DES 的攻击发明出来，后来演变成为一种针对DES 和其他分组算法的成功而有效的攻击。攻击者使用两条明文消息，并在它们经过不同的S 盒时跟踪分组上发生的变化(每条消息都以相同的密钥加密)。得到的密文中已确定的差异用于推测不同可能密钥值的概率。攻击者使用其他几组消息继续上述过程，并检查公共密钥概率值。随着加密过程中的大多数可能值都被用到，密钥也就逐渐显露出来。由于攻击者选择不同的明文消息进行攻击，因此它也是一种选定明文攻击。

⑭线性密码分析(linear cryptanalysys)。是一种已知明文攻击，利用线性近似来描述块密码的行为。如果有足够多的明文和相应密文对，便可得到有关密钥的少许信息，而数据量的增加通常会给成功带来更高可能性。

⑮彩虹表。彩虹表是对散列输出进行过分类处理的查询表，相当于密码字典的作用，提高了破解速度。

⑯因子分解攻击。以RSA 算法为目标。由于该算法用大质数的乘积生成公钥和私钥，这种攻击试图通过分解这些数的因数来找出密钥。

⑰逆向工程。这种攻击很常用。买一套同款的密码系统，反编译来分析算法找漏洞。

⑱社会工程。坑蒙拐骗、威逼利诱什么的。

六、基于编码缺陷的攻击（第三域）

①维护钩子和特权程序 Maintenance Hooks and Privileged Programs

就是后门。A maintenance hook（维护钩子）、A back door（后门）、A trap door（陷门）都是一样的。但都不是A Trojan horse（木马）。

②增量攻击 Incremental Attacks

某些攻击形式以缓慢的、渐进的增量方式发生，而不是通过明显的或可识别的活动来危害系统的安全性或完整性。对数据进行细小的、随机的或增量的改变是不容易被发现的。数据欺骗和salami 攻击就是这样的攻击形式。Salami 就是每次雁过拔毛（就薅一点羊毛）。它的另一种说法就是Data diddling（数据欺骗）。

加密的文件系统可以保证不会发生数据欺骗。对于salami 只有通过适当的责任分离和对代码的适当控制，才能完全阻止或消除，尤其是金融上要监控小额交易。

③竞争条件 race conditions ——检查时间/使用时间(TOC/TOU)

竞争条件和 TOC/TOU 攻击之间的差异是细微的，但安全专业人员必须理解它。

检查时间/使用时间：发生在多任务操作系统中，就是在两个进程中强插一个进程。如：进程 1 用来验证和授权用户，进程 2 用来调用被授权访问的这个文件；如果攻击者重定向进程 2 打开另一个涉密的文件，那么攻击者就执行了 TOC/TOU 攻击。为了避免 TOC/TOU 攻击，操作系统使用软件锁的概念，即对进程要访问的文件或资源使用一个锁，此时，这个文件不能被另外一个文件取代。

竞争条件：是 TOC/TOU 攻击的另一种形式，攻击者操纵两个进程的执行顺序，强制其乱执行。多个进程要使用同一个资源时，竞争条件就会发生。如：先验证后访问的顺序被颠倒过来。为了防止条件竞争攻击，程序应该不允许关键任务被分开执行，系统内要实现原子操作。

④高级持续性攻击(advanced persistent threat, APT)。

“震网”事件就是 APT。

特点：常用于军事，一般是一个攻击团队，具有很强的能力和技巧（高级性），资金充足，针对具体明确的特点目标，低调隐蔽择机行动（持续性）。

防御：杀毒等主机检测方法是查不出高级木马的，通常通过分析网络流量来判断，即主机有新的 IRC 连接时，则表明系统里有僵尸在尝试与外部命令中心通信。

⑤洛基攻击 Loki

Loki 攻击是今天最常用的一种隐蔽通道，这种攻击使用 ICMP 协议进行通信。Loki 工具允许攻击者紧接着 ICMP 首部之后写入数据。

⑥中间人攻击

入侵者将自己插入两台计算机正在进行的对话中，因而能够拦截并阅读它们之间来回传送的信息。使用数字签名和相互身份验证技术可以防止这类攻击。

⑦泪滴攻击

这种攻击向受害者发送畸形的分片数据包。通常，受害者的系统并不能正确地重新装配这些数据包，因此造成死机。

防止这类攻击的对策是给系统安装补丁，并使用进入过滤以检测这些数据包。

①缓冲区溢出：有很多方法创建或利用缓冲区溢出，但下面是个缓冲区溢出是如何工作的一般示例。一个是攻击目标的程序，被提供了比这个应用想处理的更多的数据。这可以通过很多方法完成，如在一个对话框中输.入过多的文本，提交一个太长的 web 地址，或创建一个比需要大得多的网络报文。被攻击的程序(目标)溢出了分配给输入数据的内存并且把超出的数据写入了系统内存。过量的数据可能包含机器语言指令，这样当下一步执行时，攻击代码，像 Trojan 木马或其它类型的恶意代码，就会运行。(经常地，多余数据的靠前部分包括被 CPU 读做“无操作”(NOP)的字符，形成一个“NOP”雪橇。恶意代码通常在多余数据的末尾。

实际的攻击方法更为详细且高度依赖目标操作系统和硬件架构。追求的结果就是把攻击代码放入到内存。这些指令通常做一些，诸如以一定方式给内核打补丁来在一个提升的权限级别执行另一个程序的事情。有时，恶意代码将调用其他程序，或甚至从网络上下载它们。

②全民程序员：由于台式和个人计算机(甚至应用程序，现在)都配备了脚本和编程工具，允许所有计算机用户创建他们自己的工具是一种常见的做法。这可能产生极其有害的后果并且

可能违反职责分离的原则。如果允许这种未被监管的编程，那么一个单独的用户可能完全控制一个应用或过程。虽然传统上程序员很少或没有接受过安全需求培训，他们至少也要对软件质量，可靠性和互操作性的问题有基本的了解。普通用户没有这样的培训并且可能创建安全和可靠性都有问题的应用。Visual Basic，包含在 lvlicrosoft Office 套件中，经常被全民程序员用来开发他们的应用或扩展一个存在的应用。公民，或普通的，程序员不可能经过系统开发实践培训或约束，其涉及正确的应用设计，变更控制，和应用的支持。因此，以这种方式开发应用可能是混乱的并且缺少对安全的任何形式的保证。在需要的时候，它应该作为策略，执行，意识，和约束的问题解决。

③隐蔽信道：一个隐蔽信道或限制问题是一个信息流问题。它是一个通信信道，允许两个协作的进程以违反系统的安全策略的方式传递信息。即使已经存在保护机制，如果未授权的信息可以通过信号机制在实体或对象之间传递，其通常被认为不能通信的，那么一个隐蔽信道可能存在。用简单的术语，它是任何的信息流，故意的或无意的，它使一个没有这个信息、的授权的观察者，可以去推断它是什么或它的存在。这在包含高度敏感信息的系统中是重要的问题。通常定义的隐蔽信道类型有两类：存储和时间。

一个隐蔽存储信道涉及一个进程直接或间接读取存储位置同时另外一个进程也在直接或间接地读取相同的存储位置。通常，一个隐蔽存储信道涉及有限的资源，例如内存位置或磁盘上的扇区，其被在不同安全级别的两个主体共享。

一个隐蔽时间信道取决于能够影响一些其他进程能获取资源的速率，例如 CPU，内存，或 I/O 设备。速率的变化也许可以用来传递信号。本质上，把信自、的传递给其它进程的进程调制它自己对系统资源的使用，以这样的方式进行，这个调制影响了第二个进程观察到的真实的啊应时间。通常认为时间信道没有存储信道效率高，因为它的带宽减小了，但它们通常更加难以检测和控制。

这些例子只与一种情景相关，其中一个内部人员试图给外部人员提供信息且在应用中受到很大限制。为了对隐蔽信道有一个全面的见解应该设想一个更广泛的概念，它包括，例如，无意的隐蔽信道，其使一个未明或未授权的人员可以观察一个系统的活动，其使一个不应该知道的人可以推理事实。

④格式不正确的输入攻击：目前已知，一些攻击利用来自用户的输入，并且各个系统检查和防范此类攻击。因此，一些新的攻击依赖于以不寻常的方式配置那个输入。例如，一个攻击，其将 web 浏览器重定向到另外一个站点，可能被防火墙通过检测一个不当站点的统一资源定位符(RUL)而捕获。然而，如果该 URL 用 Unicode 编码而不是 ASCII，防火墙可能会无法识别这个内容，而 web 浏览器则很容易地转换这个信息。

在另一种情况，很多站点允许请求访问数据库，但在请求上放置过滤器来控制访问。当允许请求使用结构化查询语言(SQL)时，在查询中使用某些特定语法结构可能骗过过滤器，其把查询看成了注释，于是查询可能提交到数据库引擎并且取回比所有者允许的更多的信息。在另一个例子中，一个站点允许用户输入信息让以后其他用户检索，例如一个博客，当输入以活动脚本的形式时，可能无法检测到。这是跨站脚本攻击的基础。(缓冲区溢出也是格式不正确输入的一种。)

⑤内存重用(对象重用)：内存管理涉及分配给一个进程一段时间内的内存段，然后取消分

配，然后重新分配给另一个进程。因为残留的信息可能保持，当之前的进程用完它之后，一个内存段可能被重新分配给一个新进程，一个安全违反可能出现。

当内存被重新分配后，操作系统应该确保内存被彻底清零或完全写覆盖，在它在能被新进程访问之前。因此，内存中没有残留信息从一个进程带到另外一个进程。在这方面内存位置是首要关心的问题，开发者也应该小心重用其它可能包含信息、的资源，例如磁盘空间。磁盘上的分页或交换文件经常得不到保护，如果没有小心地采取保护，可能包含大量的敏感信息。

注意，内存或对象重用可能是隐蔽信道的一种形式，如前面所讨论。

⑥可执行内容/移动代码：可执行内容，或移动代码，是一种软件，它从远程源通过网络传输到本地系统，然后在本地系统上执行。代码的传输是由用户的行为触发的，在某些情况下，没有用户明确的行动。该代码可能作为电子邮件的附件或通过网页到达本地系统。

移动代码有很多名称：移动代理，移动代码，可下载代码，可执行的内容，活动的胶囊，远程代码等。尽管词语似乎是相同的，但也有细微的差别。例如，移动代理是可以从主机迁移到网络中的主机的程序，有时可能是它们自己选择的位置。它们高度自治，而不是直接地受控于一个中心点。移动代理不同于小程序，它们是作为用户的操作结果而下载的程序，之后从头到尾都是在一个主机上执行。例子包括 ActiveX 控件，Java 小程序，和运行在浏览器中的脚本。所有这些都与远程源代码在本地执行相关。

七、针对网络的攻击（第四域）

1.DoS 和 DDoS/ denial-of-service

拒绝服务攻击是一种资源消耗型攻击，它以阻止受害系统的合法活动为主要目标。DoS 不是一个单一的攻击，而是指一类攻击。一些攻击利用操作系统软件的缺陷，而其他的则把重点放在安装的应用程序、服务或协议。一些攻击利用具体的协议，包括互联网协议 IP，传输控制协议 TCP，lnternet 控制消息协议(ICMP)和用户数据报协议 UDP 等。

靠一台主机攻击显然力量不够，最好是 DDOS，通过僵尸网络来搞，还能隐藏自己。

怎么防 DOS 不说了，应该都想得到。考试中有使用 tarpit 来防御 DOS，类似于蜜罐，是一个模拟的有漏洞的服务组件，当遭受一些非法扫描等攻击时，它会让攻击者的自动扫描的工具软件出现响应失败或连接超时。

2.偷听/窃听 Eavesdropping

窃听需要搭线。由于使用的是被动攻击方式，因此检测偷听设备和软件通常较为困难。如果偷听或窃听从而更改通信数据或在其中添加数据，则属于主动攻击类型。Sniffers、NetWitness、T-Sight、Wireshark、Zed Attack Proxy (ZAP)等好多工具可以用。

保证在内部基础架构之外安全可靠地传输数据是极其重要的，就是要加密。

3.假冒/伪装 Impersonation/Masquerading

模仿或是伪装，是一种假装是某人或假装是某物并获得未经授权而访问系统的行为。这通常意味着认证证书被窃取或者遭受篡改并满足(即成功地绕过)认证机制。这不同于欺骗，实体提出了一个虚假的身份但没有任何证据(如错误地使用 IP 地址、MAC 地址、电子邮件地址、系统名称、域名等)。模仿往往可以通过捕获网络服务会话设置中的用户名和密码加以实现。

对付假冒攻击的解决方案包括：使用一次性填充和令牌身份验证系统，使用 Kerberos ，

使用加密，从而增加从网络通信中提取身份验证凭证的难度。

4.重放攻击 Replay Attacks

重放攻击是假冒攻击的一种，它可以利用通过偷听捕获的网络通信进行攻击。重放攻击企图通过对系统重放被捕获的通信来重建通信会话。你可以使用一次性身份验证机制和序列化会话身份标识来防范重放攻击。

5.修改攻击 Modification Attacks

能够更改被捕获的数据包，然后再将其放回到系统中。被修改的数据包被设计为能够避开改良的身份验证机制和会话排序的限制。针对修改重放攻击的对策包括数字签名验证和数据包校验和验证。

6.地址解析协议欺骗 Address Resolution Protocol Spoofing

ARP 用于通过轮询使用系统的 IP 地址来发现该系统的 MAC 地址。对付 ARP 攻击的手段包括：为关键系统定义静态的 ARP 映射，监控 ARP 缓存中的 MAC-TP 地址映射，或者使用 IDS 检查系统通信中的异常以及 ARP 通信中的变化。

7. DNS 投毒、欺骗和劫持 DNS Poisoning, Spoofing, and Hijacking

详细的不想讲了，在第三域的 E.1 章节讲了。

8. 超链接欺骗 Hyperlink Spoofing

与 ARP 相关联的另一种攻击是超链接欺骗。这种类似于 DNS 欺骗的攻击用于将通信重定向至欺诈系统或冒名系统，或者简单地将通信发送至预定目的地之外的任何地方。超链接欺骗既可以采用 DNS 欺骗的形式，也可以只是简单地在发送给客户端的文档的 HTML 代码中修改超链接 URL，因为大多数用户并不通过 DNS 验证 URL 中的域名，而是认定超链接是合法的并进行点击，所以超链接欺骗攻击往往都会成功。

网络钓鱼(phishing)是另一种经常使用超链接欺骗的攻击。网络钓鱼意味着诱骗他人上钩，从而获得信息。这种攻击可以采用很多形式，包括使用伪造的 URL。

9.泛洪 flooding attack

泛洪这个词一点都不好听，也不知道是谁在什么时候发明的，洪泛这个词是错的。泛洪就是泛滥的意思，也有教材说泛洪是交换机和网桥使用的一种数据流传递技术，将某个接口收到的数据流从该接口之外的所有接口发送出去。如果数据帧中的目的 MAC 地址不在 MAC 地址表中，就要向所有端口转发，请示回应。泛洪攻击有以下几种：

①SYN 泛洪。利用 TCP 的三次握手机制，有两种：PING 包泛洪就是向目的大量 PING，死亡之 PING；smurf 就是向网络发大量改了回应地址的 SYS 包，让主机（或僵尸网）都把响应包发送给目的机。

②DHCP 泛洪。

③ARP 泛洪。

④UDP 泛洪。

10.VLAN 攻击

下面给出针对 VLAN 在数据链路层的最常见的攻击：

①MAC 洪泛攻击：这是不典型的网络“攻击”，但会限制所有交换机和网桥的工作方式。如果交换机的 ARP 地址映射表已满，地址不再被学习，则流量将被永久进行(来源口)端口泛洪

(portsflooding)。

②802.1Q 和交换链路间协议(ISL)标记攻击：标记攻击允许在一个 VLAN 中的用户获得未经授权的访问权限，来访问另一个 VLAN。例如，如果一个 Cisco 交换机端口被配置为动态中继协议(DTP)收到了假 DTP 包，它可能成为一个中继端口，并接受另外一个 vlan 的流量。这通常被称为“VLAN 泄漏”。这可以通过设置关闭所有非 DTP 信任端口进行防范，也可以通过简单的配置指南或软件的升级来防范。

③双封装 802.1q/nested VLAN 攻击：在交换机内，VLAN 号码和识别信息是放置在一个特殊的扩展格式，允许转发路径保持端到端隔离 VLAN 不丢失任何信息。ISL 是 Cisco 专有技术，在某种意义上是一个紧凑的扩展报头。一个 VLAN，没有明确对一个 802.1Q 链路相关的任何标签。这个 VLAN 是隐式用于一个 802.1Q 端口收到的所有未标记的通信能力。这种能力是可取的，因为它允许 802.1Q 端口能够与旧的 802.3 端口直接发送和接收数据流量。当双封装 802.1 Q 包注入到网络设备的 VLAN 是一个 TRUNK 的 native VLAN 时，这些数据包的 VLAN 标识不能从端到端保存，这是因为 802.1Q TRUNK 总是通过剥离外层标签修改数据包。在外部标签去除后，内部标签只有数据包的 VLAN 标识符。区此，采用两个不同的标签双封装数据包，流量可以跨越 VLAN。

④ARP 攻击：不说了。ARP 中毒或 ARP 欺骗还有中间人攻击什么的。

⑤组播暴力攻击：这种攻击试图利用交换机的潜在漏洞，发起二层多播帧的风暴。正确的行为应该是限制源 VLAN 的通信流量，不当的行为会泄露帧到其他 VLAN。

⑥生成树攻击：另一种攻击，试图利用可能的交换机的弱点发起 STP 攻击。攻击需要在链路上，嗅探得到 STP 帧，得到端口上开启的 STP ID，然后，攻击者会发送 STP 的配置/拓扑变化确认 BPDU，宣布他是一个很低的优先级的新根桥。

⑦随机帧暴力攻击：这最后的攻击，可以有很多形式，但总的来说是蛮力攻击，随机变化的一个或几个数据包字段，而保留了源地址和目的地址，等常数信息。

11.战争拨号

由于调制解调器几乎允许从任何地方远程访问网络，往往作为攻击者进攻网络的门户入口。使用自动拨号软件，攻击者可以拨号来识别那些是公司的调制解调器。如果与该调制解调器连接的主机，使用一个弱密码，那么攻击者可以很容易地访问网络。更糟糕的是，如果语音和数据共享同一网络.那么语音和数据可能都被破坏。

最好的防御这种攻击的方式是，要确保所有的调制解调器使用双因素认证。

八、针对访问控制的攻击（第五域）

1.访问聚合攻击 Access Aggregation Attacks

通过收集多个非敏感信息块，并将他们结合来获得敏感信息。（第三域，E.3 章节里的数据库安全里，已经讲了聚合攻击和推理攻击）。网络侦察(Reconnaissance)就是是访问聚合攻击，结合多种工具来识别系统的多个元素，如 IP 地址、开放端口、运行服务、操作系统等等。

应结合严格访问控制、“需知”和最小特权原则来预防聚合攻击。

2.密码攻击 Password Attacks

破了管理员密码或特权密码，也就得到了一切。所以很多单位都要求必须设置“强密码”。

①字典攻击 Dictionary Attacks

密码攻击的一种，比暴力破解快此地，但必须要有好的字典。此外，字典式攻击经常会扫描差别构建式密码。一个差别构建式密码是之前使用过的密码，但有一个字符的不同。例如，password1 是 password 更改一个字符后的密码，其它的如 Password、lpassword 和 passXword 也是。攻击者在生成彩虹表时经常使用这种方法。

②暴力攻击 Brute-Force Attacks

密码攻击的一种，通过尝试所有可能的字母、数字和符号组合来发现用户帐户的密码。密码越长，计算量就越大。还有一种常用的方法是：散列值匹配查找。因为密码都不会在网络上发送，传输和存储的都是其散列值，所以只要能找到 1 个散列冲突（碰撞）collision，就可以实现登陆破解了。要破解散列值，就要用到生日悖论和彩虹表了。

③生日攻击 Birthday Attack

第三域 I.8 章节已经讲过生日悖论了。如果把 23 个人关在一个房间，那么任何两人同一天生日的可能性有 50%；如果有 367 人在一个房间里，你会有 100%的机会获得至少两个有相同生日的人。MD5 已经被破解了，SHA-3 目前还是安全的。

④彩虹表攻击 Rainbow Table Attacks

彩虹表预先计算好的各种字符串和散列值的映射数据库。使用 4 种字符类型的 14 位字符长度的密码的散列的彩虹表大约是 7.5GB 大小。这不大吧，可以大幅加快密码破解速度。

许多系统一般通过“加盐”密码来减少彩虹表攻击的有效性。盐是一组随机位，在散列前加到密码中。加密方法在散列前就加入附加位，这样随机性更大了，使攻击者更难以使用彩虹表密码

⑤嗅探攻击 Sniffer Attacks

一个嗅探器(也称为数据包分析器或协议分析仪)是)个软件应用程序，通过网络捕捉和分析流量。Wireshark 是一种受欢迎的协议分析器。

3.电子欺骗攻击 Spoofing Attacks/masquerading

电子欺骗(即伪装)是指假装成某物或某人等。电子欺骗的种类很多，有 IP 欺骗、邮件欺骗、电话欺骗等等。

4.社会工程学攻击 Social Engineering Attacks

社会工程不难，但每次考试都会出几道题！社会工程就是与人斗，其乐无穷。

①网络钓鱼 Phishing

钓鱼邮件告知用户虚假信息，然后就能骗到有用的信息，或者实现木马植入。

②鱼叉式钓鱼 Spear Phishing

针对特定用户组的钓鱼方式。

③捕鲸 Whaling

捕鲸是的目标是大鱼、高层或高管。

④语音钓鱼 Vishing

纯属忽悠，就能搞定。

5.智能卡攻击 Smartcard Attacks

各种途径搞定卡的信息。

①故障生成(fault generation)攻击

攻击者通过操纵智能卡的一些环境组件(改变输入电压、时钟频率、温度波动)来引入这些“错误”。在向智能卡引入一个错误之后，攻击者会检查某个加密函数的结果，并查看没有出现错误时智能卡执行该函数得到的正确结果。分析这些不同的结果使得攻击者能够对加密过程进行反向工程，并有望获得加密密钥。这种攻击也称为故障生成攻击。

②旁路攻击(side-channel attack)

是非入侵式攻击，并且用于在不利用任何形式的缺陷或弱点的情况下找出与组件运作方式相关的敏感信息。针对智能卡的差分功率分析(differential power analysis，查看处理过程中的功率发射)、电磁分析(electromagnetic analysis. 查看发射出的频率)和计时(完成特定过程所需的时间)都是旁路攻击的示例。

③微区探查(microprobing)

使用针头和超声振动去除智能卡电路上的外部保护材料，随后就可以通过直接连接智能卡的 ROM 芯片来访问和操纵其中的数据。

九、分析攻击汲取经验（第七域）

1.拒绝式服务攻击 Denial-of-Service Attacks

拒绝服务(DoS)攻击能够阻止系统处理或响应来自资源和客体的合法数据或请求。拒绝服务攻击的最常见形式是向服务器传输使其无法全部处理的过多数据包，或让系统崩溃或 100%的 CPU 使用率。另一种形式的 DoS 攻击是一种分布式拒绝服务(DDoS)攻击。还有一种变体的 DoS 形式被称为分布式反射拒绝服务(DRDoS) distributed reflective denial-of-service，域名服务(DNS)投毒攻击和 smurf 攻击就是这样的例子。

2.SYN 泛洪攻击 SYN Flood Attack（让你回不停）

SYN 泛洪攻击是一种常见的 DoS 攻击。它通过破坏 TCP/IP 启动通信会话的三步握手标准来实施攻击。通常，客户端向服务器发出 SYN (同步) 数据包，服务器向客户端发送 SYN/ACK (同步/应答)响应数据包，随后客户端向服务器回应 ACK (应答)数据包。这样三步握手建立起了两个系统间的一个用于数据传输的会话，这个会话直到出现 FIN (结束)或 RST (重置)包才会断开。然而，在一个同步字符(SYN)洪水式攻击发生时，攻击者发送成千上万个 SYN 包但不回复响应。这类似于一个喜欢开玩笑的人伸出手去握手，但是当其他人做出回应，伸出手准备握手时，他却将手缩了回来，留下对方的手悬在半空中。

使用 SYN Cookies 是阻断这攻击的一种方法。这些小记录消耗小部分系统资源，当系统接收到 ACK 应答肘，它检查 SYN Cookie 并建立会话。防火墙通常能够通过入侵检测和入侵防御系统检测 SYN 攻击。阻断这种攻击的另一种方法是降低 TCP 重置攻击服务器通常会等待一段时间以接收 ACK 应答。默认时间是三分钟，但在正常操作中合法系统发送 ACK 应答并不需要这么长的时间。通过减少时间，半开的会话在系统内存中的刷新会更快。

3.TCP 重置攻击 TCP Reset Attack（让你连不上）

另一种通过操纵 TCP 会话的攻击方式叫做 TCP 重置攻击，会话通常是 FIN(完成)或 RST(复位)包。攻击者可以在一个 RST 包中伪造源 IP 地址并断开会话活动。两个系统之间则需要重新建立会话。这对系统来说是一个很大的威胁，两系统之间需要持续的会话，以保持数据。当

会话重建时，系统就需要重建数据，所以这不仅仅只是来回发送三个数据包以建立会话的问题。

4.Smurf 和 Fraggle 攻击（前者反弹、后者 UDP）

Srnurf（欺骗）和 Fraggle（磁片）攻击都属于 DoS 攻击。Smurf 攻击是另一种类型的洪水式攻击，但它使用 Internet 控制消息协议(ICMP) 回送数据包而不是 TCP SYN 包攻击其他系统。更具体地说，它是一个使用受害者的 IP 地址作为源 IP 地址的伪造广播 ping，让全网都响应并回送数据包至受害 IP。在 1999 年发行的 RFC 2644 改变了路由器的标准，路由器不能转发定向广播，网络便不能被放大。这给 Smurf 攻击单一的网络带来了限制。此外，在防火墙上禁用 ICMP 能够防止利用 ICMP 的任何类型的攻击。现在 Smurf 攻击已经很少见了。

Fraggle 攻击类似于 Smurf 攻击。然而，Fraggle 攻击使用 UDP 端口 7 和 19 而不是 ICMP。Fraggle 攻击能够使用伪造 IP 地址将一个 UDP 数据包发送给受害者。所有的系统就都会将其转发给受害者，这类似于 Smurf 攻击。

SMURF 是反弹攻击，消耗带宽（ICMP）；FRAGGLE 消耗性能（UDP）。

5.Ping 洪水攻击（呼死你）

Ping 洪水攻击，通过给受害者发送洪水般的请求来达到攻击目的，在 DDOS 攻击中给僵尸网络发送僵尸信息的效果很明显。如果成千上万的系统同时给一个系统发送 ping 请求，该系统将在试图回答 plng 请求时发生混乱。

6.僵尸网络 Botnets

今天僵尸网络相当普遍。僵尸网络中的计算机就像机器人(通常称为僵尸 zombies，也叫肉机)，并将会按照攻击者的要求执行命令。僵尸牧人 bot herder 通常是指通过一个或多个命令控制所有计算机和服务器的罪犯。

7.死亡之 Ping/Ping of Death（PING 大包）

一个 ping 死亡攻击采用了一个超大的 ping 数据包，即超过 64 字节，甚至大到 64KB。当系统收到 ping 包大于 64 KB 时，就会出现问题。现今死亡 PING 攻击很少能够成功，因为补丁和更新改善了系统的脆弱性。

8.泪滴攻击 Teardrop（拼不完整）

在泪滴攻击中，攻击者阻碍交通，系统无法将数据包一起发回。大数据包通常被分成较小的碎片，当它们被发送到网络上时，接收系统把数据包碎片还原到原来的状态。然而，泪滴以一种系统不能将文件还原在一起的方式分割数据包。旧的系统无法处理这种情况，并会崩溃，但补丁解决了这个问题。此外，入侵检测系统可以检查畸形数据包。

7.Land 攻击（自己搞自己）

Land 攻击是指攻击者使用受害者的 IP 地址作为源 IP 地址和目的 IP 地址，并发送伪造的 SYN 包给受害者。这使系统不断地对自己做出应答，并最终可能会冻结，崩溃或重新启动。这种攻击在 1997 被第一次发现，它又几次攻击不同的端口。保持一个系统更新并使用过滤流量检测相同的源和目的地地址，有助于防止 Land 攻击的发生。

8.零日攻击 Zero-day Exploit

零日漏洞是指利用他人未知的系统漏洞对系统发起攻击，也指无法修补的漏洞。

9.恶意代码 Malicious Code

恶意代码是指在计算机系统上执行不必要的、未经授权的或未知活动的脚本或程序。恶意

代码可以采取多种形式，包括病毒，蠕虫，木马，具有破坏性宏的文件，和逻辑炸弹。它通常被称为恶意软件，或恶意代码。恶意代码存在于每一种类型的计算机或计算设备，是现今最常见的安全漏洞。

10.中间人攻击 Man-in-the-Middle Attacks

当一个恶意用户能够在一个正在进行的通信的两个端点之间的逻辑上获得一个位置时，一个中间人攻击就会产生。中间人攻击有两种。一个涉及复制或刺探双方通信，这基本上算是嗅探器攻击；另一种类型是攻击者在通信线上定位自己，他们将其作为一个存储和转发或代理机制，客户端和服务器认为它们是直接连接的。攻击者可以收集登录凭据和其他敏感数据，以及改变两个系统之间交换的消息内容。

中间人攻击比其他许多攻击需要更多技术性，因为从客户角度出发，攻击者需要冒充服务器，从服务器的角度来看，还要模拟客户端。中间人攻击往往需要一个组合的多个攻击。例如攻击者可能会改变路由信息和 DNS 的值，或伪造地址解析协议(ARP)查找。

11.战争拨号 War Dialing

使用调制解调器搜索接受入站连接尝试的系统的行为，就是大量拨号。一旦检测到某个计算机载波音，战争拨号器就会在搜索过程结束时所生成的报告中添加相应的电话号码。一种新的战争拨号的形式能够在不适用调制解调器的情况下，使用语音互联网协议(VoIP)拨号，这使得攻击者能够扫描到更多的电话号码，并发现除了调制解调器以外的其他设备，如传真机、语音信箱、拨号音和人类的声音。

抵御恶意战争拨号攻击的对策包括：实施强大的远程访问安全性(主要依靠强的身份验证)，确保不存在未授权的调制解调器，以及使用回叫安全机制、协议约束与呼叫登入。

12.破坏 Sabotage

员工破坏指的是员工对单位的破坏行为。员工被解雇后必须立即终止或禁用其账户，预防员工破坏的其他保障措施还存定期审计、监测异常或未经授权的活动，保持员工和管理人员之间的沟通开放，并适当奖励员工。

13.间谍 Espionage

间谍活动是一种收集专有的、秘密的、私人的、敏感的或机密信息的恶意行为。

十、针对数据库的攻击（第八域）

1.聚合 Aggregation

聚集攻击是通过收集大量的低安全级别的或低价值的数据，将它们结合起来，创造较高安全级别或有价值的信息。对于数据库来讲，就必须严格控制对聚合函数的访问并且充分估计可能展示给未授权个体的潜在信息，这些对数据库安全管理员来说是特别重要的。

SQL 就供了许多可从一个或多个表中组合记录并生成有用信息的函数包括 count，mm，mate，sum，avg 等，这一过程就是聚合。数据库管理员应该严格控制聚合函数的访问，并且可以使用视图(view)的访问方式。防范聚合的对策有：

①基于内容的访问控制(Content-dependent access control)：根据数据本身的敏感度来管理访问控制。

②数据库分区技术可以防止聚合和推理。每个分区都具有唯一的、不同安全级别的内容。

③视图可以防止聚合攻击。在数据库中实现多级安全性的一种途径是使用数据库视图。视图可以整理来自多个表的数据、聚合单独的记录或限制用户访问数据库属性和/或记录的有限子集。在数据库中，视图被存储为SQL语句，而不是被存储为数据表。这样可以减少所需的数据库空间，并且允许视图违反应用于数据表的规格化规则。因为视图非常灵活，所以许多数据库管理员将视图作为一种安全工具使用，就是允许用户只与受限的视图交互，而非与作为视图基础的原始数据表交互。

④结合严格访问控制、“需知”和最小特权原则来预防聚合攻击。

2.推理 Inference

推理与聚合有点像，推理攻击利用几个非敏感信息片的组合，从而获得对应该属于更高级分类的信息。推理需要利用人的推断能力，而聚合只是简单的叠加。对于推理攻击的最好的防范是对有特权的个人用户保持持续的警惕。此外，数据的故意混淆可以被用来防止对敏感信息的推理。最后，你可以使用数据库分区帮助降低这些攻击。防范推理攻击的方法有：

①单元抑制(cell suppression)：隐藏特定存储单元的内容，限制用户对特定内容的访问。

②数据库分隔/分区(database partition)：把数据库逻辑分区，用视图来提供访问。

③噪声与扰动(noise and perturbation)：在数据库中插入伪造信息，误导和迷惑攻击者。

④基于上下文的访问控制(Contest-dependent access control)：根据访问的状态或者顺序来限制对某些内容的访问，需要一定的学习功能。

⑤基于内容的访问控制(Content-dependent access control)：根据数据本身的敏感度来管理访问控制。（信息分级）

⑥多实例（Plolyinstantiation）在同一个关系数据库表中两行或更多行（无组）具有相同的主键，且为不同密级的用户提供不同的数据查询结果，就是多实例。主要防范推理攻击。（这个点经常考到）

③旁路攻击

用户试图绕过数据训应用的前端控制访问数据。

④并发

并发相关的问题包括使用旧数据执行过程，不一致的更新，或发生死锁。

⑤死锁

当两个用户同时访问信息而且都被拒绝时就发生死锁。

⑥攻击数据库视图以非法访问

用户可能试图受限视图或修改一个已经存在的视图;在数据库接口设计中经常使用的分层模型提供了一个相同数据的多条路径，不是所有的路径都受到保护。

⑦拒绝服务

任务类型的可以阻止授权用户共聚信息的攻击或行动。

⑧不当信息修改

未授权或授权用户可能故意或无意的错误地修改信息。

⑨查询攻击

用户尝试使用查询工具来访问不能正常地通过可信前端访问的数据。

⑩服务器访问

数据库运行的服务器必须防止未授权的逻辑访问同时也要防止未授权的物理访问以防止逻辑控制被禁用。

⑾数据污染

由于输入数据错误或错误的处理导致的数据完整性破坏。

⑿数据拦截（中间人）

如果允许拨号或其它类型的远程访问，必须控制拦截会话或修改传输中的数据的威胁。

⒀检查时间 / 使用时间(TOC/TOU)（必考）

TOC/TOU 也可能发生在数据库中。一个例子是，一些类型的恶意代码或特权访问可以改变数据，在用户的查询被许可时和数据展现给用户时。

⒁未授权访问

故意可无意地将信息发布给未授权用户。例如系统的错误消息或系统提示，提供了关于服务功能特性等方面的信息。

要实现多种等级的数据库访问控制和安全防护，有很多方法：

①使用视图 Views

视图可以防止聚合攻击。在数据库中实现多级安全性的一种途径是使用数据库视图。视图可以整理来自多个表的数据、聚合单独的记录或限制用户访问数据库属性和/或记录的有限子集。在数据库中，视图被存储为 SQL 语句，而不是被存储为数据表。这样可以减少所需的数据库空间，并且允许视图违反应用于数据表的规格化规则。因为视图非常灵活，所以许多数据库管理员将视图作为一种安全工具使用，就是允许用户只与受限的视图交互，而非与作为视图基础的原始数据表交互。

②并发性 Concurrency

并发性使用“锁定”功能来允许已授权用户更改数据，同时拒绝其他用户访问查看或更改数据元素。只有更改完成并“解锁”后，才允许其他用户访问。并发性或编辑控制是一种预防性的安全机制，这种机制试图使数据库中存储的数据始终是正确的，或者至少使其完整性和可用性受到保护。

③语义完整性 Semantic integrity

语义完整性是 DBMS 的一种常见安全特性，确保用户的动作不会违反任何结构上的规则。此外，还检查所有存储的数据类型都是有效的，符合逻辑的，并且确认系统遵守任何和所有的唯一性约束。

④时间戳 Time stamp

通过标记日期和时间来维护数据的完整性和可用性。

⑤细粒度控制 granularly

DBMS 的另一个常见安全特性是在数据库内能够细粒度控制对象。例如：内容相关的访问控制（基于内容）Content-dependent，分析内容之间的关系来阻止用户访问与他无关的数据，或者有利益冲突的数据。

⑥单元抑制 cell suppression

对单独的数据库字段或单元隐藏或强加更安全的约束。

⑦上下文相关的访问控制（基于上下文环境）Context-dependent

上下文相关的访问控制通过宏观评估来制定访问控制策略，它分析每个对象、数据包或字段如何与总体的活动或通信相联系，在较大的上下文环境中就会表露出是有益的还是有害的。

⑧数据库分区 database partitioning

数据库分区技术可以防止聚合和推理漏洞。

⑨多实例 Polyinstantiation

在同一个关系数据库表中两行或更多行具有相同的主键，且为不同密级的用户提供不同的数据查询结果，就是多实例。主要防范推理攻击。（这个点经常考到）

⑩噪声和干扰 false or misleading data

在 DBMS 中插入错误的或伪造的数据，从而重定向或阻挠窃密攻击。但一定要确保插入到数据库中的噪声不影响业务运营。

⑪锁控制

锁用来控制读和写访问特定的关系系统中的数据行或面向对象系统中的对象。可以在表，行，记录，或甚至字段上加锁，这些相关的要求也被称为 ACID 测试。

十一、针对软件开发的攻击（第八域）

客户端都要通过发送指令、表单什么的请求 WEB 服务，必须要对 WEB 输入的内容进行验证，不然会因为输入一些特殊字符而被攻击。如：

1.路径/目录遍历(Path or directory traversal)：这个攻击又被称为“点-点-斜线”、“../”dot dot slash；在 URL 中接入几个“../”就可以访问上级的文件目录了。

2.统一代码编码(Unicode encoding)：Unicode 是一种行业标准，开发他的目的是为了以标准的编码格式来表示世界上的 10 万多个文本字符。Web 服务器通过 Unicode 来支持不同的字符，在 Unicode 下，攻击者不用“../”来攻击，而使用 Unicode 的“%C1%lc，%c0%9v，and %C0%af”来攻击。

3.网址编码(URL encoding)：在 URL 中，“空格“表示为“%20”，其实其它字符也可以在 URL 里用特殊的方式来发送。

4.客户端验证(Client-side validation)：是指将指令发送到服务器之前在客户端进行验证，如果黑客劫持攻击者环境，插入恶意数据，也就绕过了这个验证了。

1.缓冲区溢出 Buffer Overflows

输入内存的数据太大，就会“溢出”其存储空间（编程函数先定义一个变量 var 什么的，执行时操作系统会给程序一个内存空间的），溢到隔壁的存储空间里，可能被正常执行了或影响别的进程了。利用缓冲区溢出漏洞可以在服务器上执行任意代码。

许多编程语言对变量的长度不强制实施限制，这就要求编程人员对代码进行边界检查。只要允许用户输入程序变量，编程人员就应当采取有效措施，确保满足下列各项条件：

①用户输入的值的长度不能超过任何存放它的缓冲区的大小。

②用户不能向保存输入值的变量类型输入无效的值。

③用户输入的数值不能超出程序规定的参数操作范围。

如果没有执行对上述条件的简单检查，那么就可能造成缓冲区溢出漏洞。

2.检验时间/使用时间攻击 Time of Check to Time of Use（必考）

也称为异步攻击(asychronous attack)，有的人把竞争条件（race condition）也看作是这种攻击，其实是不一样的，竞争条件是改变进程的顺序（排序）；TOC/TOU 是进入 2 个进程之间进行更改（插队）。

检验时间到使用时间(time-of-check-to-time-of-use，TOCTTOU 或 TOC/TOU)是一个时间型漏洞，当程序检查访问许可权限的时间早于资源请求的时间时，就会出现这种问题。例如，如果操作系统针对用户登录建立了一个综合的访问许可权限列表并且在整个登录会话期间查询这个列表，那么就存在 TOC/TOU 漏洞。如果系统管理员取消了某个特殊的权限，那么这个限制只有在用户下次登录时才会起作用。如果在用户登录的时候正好发生取消访问许可权限的操作，那么用户是否能够访问资源就是不确定的。用户只需保留会话打开数天之久，新的限制就永远不会被应用。

对策：系统应当使用原子操作；操作系统可以使用软件锁。

3.跨站脚本攻击(XSS) Cross-Site Scripting（必考！）

术语“跨站点脚本(Cross-Site Scripting，XSS)”指的是利用一个 Web 站点的脆弱性，在 Web 应用程序中注入恶意代码的攻击。攻击者(用客户端脚本语言，如 JavaScript)把他们的恶意代码注入到网页中。随后，不知情的用户在访问这个站点时，恶意代码就会在他们的浏览器中执行，这样可能会导致 Cookies 被盗、会话被劫持、恶意代码被执行和访问控制被绕过，或者有助于利用浏览器的错落性。XSS 攻击的关键在于将恶意代码写入 Web 站点。一般是在一个有返回结果的表单网页里，输入带<SCRIPT>标记的字段，服务器收到表单内容就会运行里面的恶意代码了。XSS 有三种类型：

①非永久/非持久性 XSS (NonpersistentXSS)，也叫反映漏洞/反射脆弱性，出现在攻击者欺骗受害者处理一个用流氓脚本来编程的 URL，从而偷取受害者敏感信息(cookie，会话 ID 等)的时候。这个攻击的原理是利用动态网站上缺少适当的输入或者输出确证。（就是返回一个有恶意代码的 URL 给用户点击）

②永久/持久性 XSS(PersistentXSS)，也叫二阶漏洞，也称为存储或者第二顺序脆弱性，通常针对的是那些让用户输入存储在数据库或其他任何地方(如论坛、留言板、意见簿等)的数据的网站。攻击者张贴一些包含恶意 JavaScript 的文本，在其他用户浏览这些帖子时，它们的浏览器会呈现这个页面并执行攻击者的 JavaScript。（就是把恶意代码存入网站）

③基于文档对象模型/DOM 型(Document Object Model based XSS)。也叫本地跨站点脚本。DOM 是标准结构布局，代表着浏览器中的 HTML 和 XML。在这样的攻击中，像表单字段和 cookie 这样的文档组件可以通过 JavaScript 被引用。攻击者利用 DOM 环境来修改最初的客户端 JavaScript。这使受害者的浏览器执行由此而导致的 JavaScript 代码。

4. SQL 注入攻击 Injection（必考！）

SQL 注入攻击比 XSS 更加危险，它同样是向 Web 应用程序输入带特殊字符的表单字段，只是它的目的不是欺骗用户，而是访问数据库。在动态网页中，经常会让用户输入附录密码、查询关键字等表单内容，然后发送给数据库进行查询或比对。如果把输入的字段加一些特殊字符，就可以让 SQL 语言执行额外的操作，从而进入数据库。比如：正解的输入密码是“123456”；要想注入就输入“123456’; XXXXX WHERE ’a’ = ’a”，那么数据库会执行 2 条正常的 SQL 语

言了。

可以通过下列三种技术来防范：

①执行输入验证。与跨站脚本攻击的防御方法一样，输入验证操作能够限制用户在表单中输入的数据类型。

②限制用户特权。Web 服务器使用的数据库账户应当具有尽可能最小的权限。

③利用数据库存储过程来限制应用程序执行任意代码的能力。存储过程就是：SQL 语句已经编写并封装好了，驻留在数据库服务器，仅可由数据库管理员修改；Web 应用程序则调用各种现成的存储过程来运行，不直接通过 SQL 语句来访问数据库。

5.侦察攻击/网络侦察扫描 Reconnaissance Attacks

目的就是找 IP、端口和漏洞。搞渗透测试必须技能，工具软件一大堆，著名的有 Nmap、Nessus，OpenVAS 什么的，应该都玩过。

6.伪装攻击 Masquerading Attacks

①IP 欺骗 IP Spoofing

很简单，防范方法是在每个网络的边缘配置过滤程序，确保数据包满足以下标准：

*内部 IP 地址的包不能从外网进入。

*外部 IP 地址的包不能从内网出去。

*私有 IP 地址的包不能过路由器。

②会话劫持 Session Hijacking

会话劫持攻击指的是攻击者中途拦截已授权用户与资源之间的通信数据，然后使用劫持技术接管这个会话并伪装成已授权用户的身份。如：

*捕获客户端与服务器之间身份验证的详细信息，并使用这些信息伪装成客户端的身份。

*欺骗客户端，使其认为攻击者的系统是与之通信的服务器，并在客户端与服务器建立合法连接的时候作为中间人（代理），断开服务器与客户端的连接。

*使用没有正常关闭连接的用户的 cookie 数据访问 Web 应用程序。

7.内存重用（客体重用）

内存被重新分配后，要清空被覆写。

其它还有：陷门/后门/维护钩子等，好多。