网络与系统安全的需求与目标

《网络与系统安全》 第二讲

首席教授： 荆继武 研究员
主讲教师： 王跃武 研究员
马 原 副研究员
助教： 郑昉昱 助理研究员

课程提纲

- 网络与系统安全的目标
- 保护阶段的需求与目标
- 全生命周期安全阶段的需求与目标
- 生存技术阶段需求与目标
- 自重构可信赖安全阶段的需求与目标

网络与系统安全的目标

- 处理信息的工具
- 保证信息安全是唯一目标
- 信息安全的需求就是网络与系统安全的需求

信息安全的需求是什么？

- 这是一个很难有确定答案的问题，因为信息技术在飞速发展。
- 最早的提法是：著名的*CIA Triad*（CIA不是中央情报局，是三个单词的首字母缩写，没有准确起源，但最确切的定义在FIPS 199）提出的信息安全核心三件套：
  - *机密性（**Confidentiality**）*
  - *完整性（**Integrity**）*
  - *可用性（**Availability**）*；
- 三个首字母的缩写CIA，被称为 *CIA Triad* 。

信息安全需求是什么？

- 2002年Donn B. Parker（ACM Fellow）在CIA三元组的基础上提出了信息安全6元素：
  - **confidentiality（机密性）**
  - **possession（可拥有性）**
  - **integrity（完整性）**
  - **authenticity（真实性）**
  - **availability（可用性）**
  - **utility（功能性）**

：CIA Triad　　：扩展内容

信息安全需求是什么？

- 2013年一篇论文提出的IAS-octave（ Yulia Cherdantseva ，2013）将信息安全的目标概括为：
  - **Confidentiality**
  - **Integrity**
  - **Availability（CIA）**
  - **Accountability（可追溯性）**
  - **Auditability（可审计性）**
  - **Authenticity/Trustworthiness（真实性）**
  - **Non-repudiation（非否认性）**
  - **Privacy（隐私）**
- 在**CIA基础上增加了5个属性**

信息安全需求是什么？

- 我们的建议：
  - 机密性： **Confidentiality**
  - 完整性：**Integrity**
  - 可用性： **Availability**
  - 真实性：**Authenticity （Trustworthy）**

其它特性可以包括在上述概念中，例如非否认性经常被认为是真实和完整性的一部分，同CIA相比主要增加了系统的真实性，

在社会分工明显的未来信息世界，信息及信息服务的真实性显得更为重要。

网络和系统如何确保信息的机密性

- **Confidentiality**：信息不能被未授权的用户（实体或者进程）知道、使用；
- 不让看：
  - 访问控制机制
  - BLP模型是优秀的机密性保护模型
- 看不懂：
  - 加密/混淆
- 看不到：
  - 隐藏

网络和系统如何确保信息的完整性

- **Integrity：数据不能被以未授权或者不可察觉的方式改动；**
- 不让乱改
  - 交易控制
  - BIBA模型是典型的保护完整性的策略
- 改了我知道
  - 系统审计
  - 检错码/纠错码
  - 数字签名

网络与系统如何确保信息的可用性

- **Availability**：确保信息在需要时是可以访问到的
- 系统与存储的可靠性
  - 系统质量
  - 容错系统
- 备份
  - 冷备份
  - 热备份
  - 冗余备份
- 分散存储与处理
  - 纠删码
  - 入侵容忍

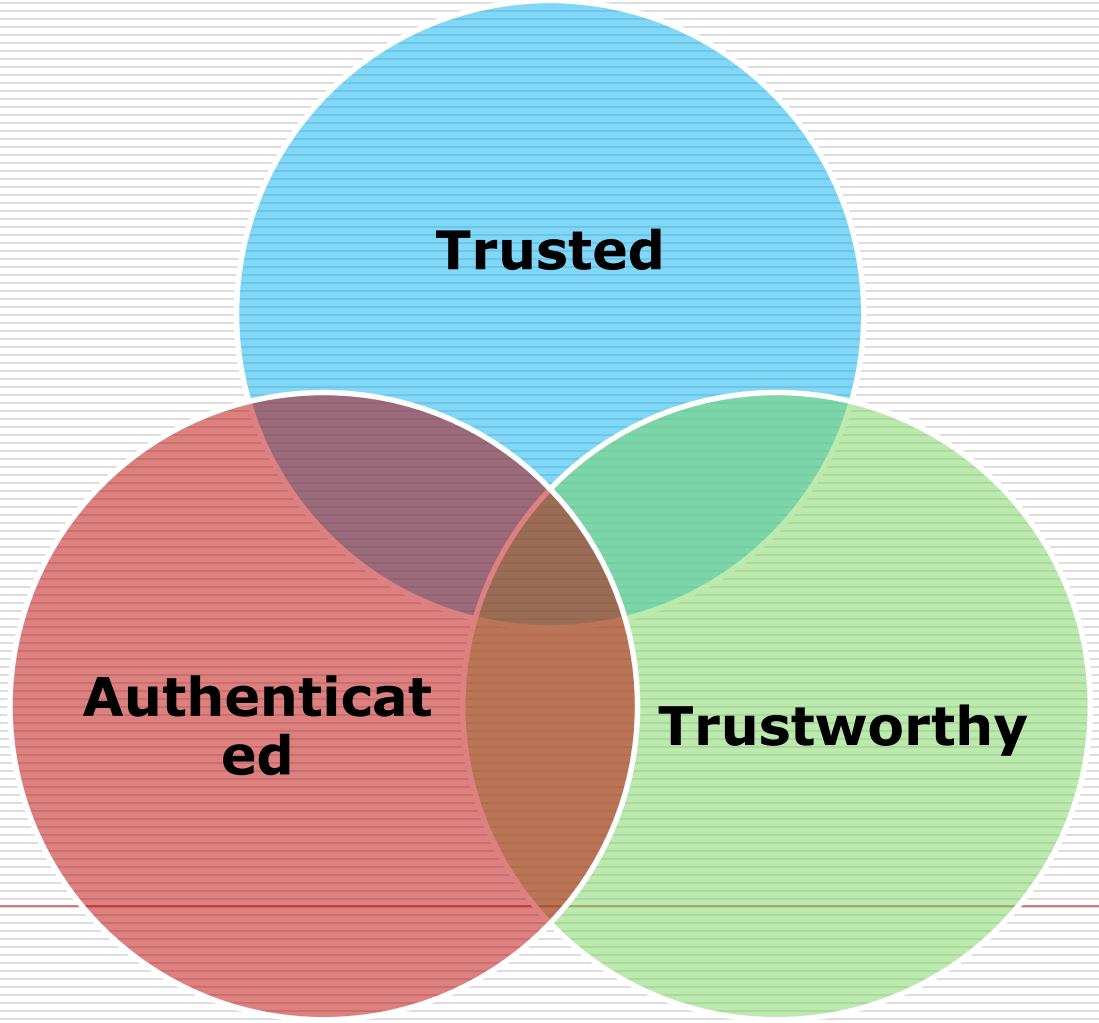
网络与系统如何确保真实性

- **Authenticity:** 可认证性，可鉴别性，真实性；
- 实体真实性
  - 计算机/设备/用户/程序/服务
- 三因素鉴别机制（静态）
  - 你知道什么/你拥有什么/你是什么
- 基于风险的真实性保障（动态）
  - 行为历史分析
  - 行为习惯分析

如何做到网络与信息安全？

- 经合组织OECD1992年提出，2002年修订的信息系统和网络安全**9**原则：
- **Awareness**（意识）
- **Responsibility**（责任）
- **Response**（反应）
- **Ethics**（道德）
- **Democracy**（民主）
- **Risk Assessment**（风险评估）
- **Security Design and Implementation**（安全设计与实现）
- **Security Management**（安全管理）
- **Reassessment**（重评估）。

区分几个单词



一些解释

- Authenticated:
  - Identification
  - Certification
  - Authorization
- Trusted
  - Trusted computing
- Trustworthy

三个概念的递进关系

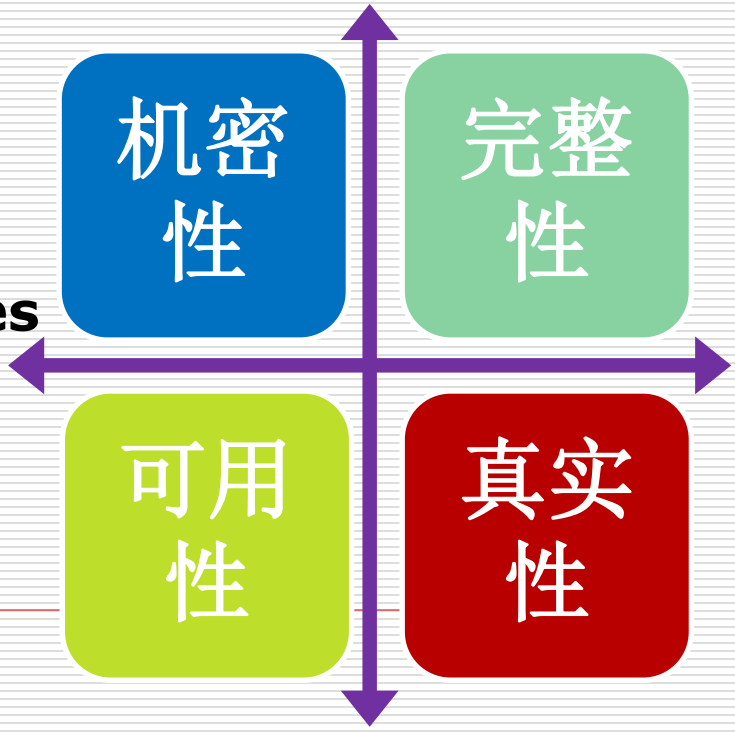

Authenticated：
系统是真实的，
Trusted：
系统是可信的
Trustworthy：
我们确信他们不会破坏安全

网络与系统安全的目标

- 网络与系统安全的目标是CIA+Authenticity
  - 系统弱点和威胁的存在使得系统安全属性难以确保

威胁：**Threats**

弱点：
vulnerabilities



弱点和威胁

- 弱点： **vulnerabilities**，系统中包含的能够被用于破坏信息安全特性的点；
- 威胁：潜在的可能造成信息破坏的任何东西；
- 系统有弱点外部有威胁。系统越复杂弱点越多

阿喀琉斯之踵是弱点，箭是威胁！

弱点和威胁

- 例子**1**. Slammer蠕虫是威胁，而SQL server中的缓冲区溢出是弱点，没有Slammer蠕虫，系统的破坏不会产生，虽然SQL Server缓冲区漏洞依然存在；
- 例子**2**. Windows98早期系统中断向量表存在可以修改的弱点，CIH病毒利用该弱点，假冒、劫持中断，直接侵入系统内核，CIH病毒是威胁，没有CIH病毒，Windows虽然有弱点一样可以运行；

网络与信息安全的目标

- **信息安全的目标为：防止威胁利用弱点破坏信息安全特性**
- **技术途径：**
  - 减少系统弱点：通过保护技术手段降低系统的脆弱点数量；（系统保护技术，设计更好的系统）
  - 管理系统弱点：识别、发现、评估系统弱点（风险分析），响应利用弱点的攻击；（全生命周期安全保护技术）
  - 降低攻击影响：在利用系统弱点攻击成功时，弱化系统功能确保使命完成（生存技术）
  - 削弱威胁成功的影响：即使敌人利用的系统弱点，也难以完成攻击（生存技术）
  - 消灭自己：没有弱点了。**夫唯不争，故天下莫能与之争**（自重构可信赖技术）

课程提纲

- 网络与系统安全的目标
- 网络与系统保护阶段的需求与目标
- 信息系统全生命周期安全阶段的需求与目标
- 信息系统生存技术阶段的需求与目标
- 自重构可信赖安全阶段的需求与目标

网络与系统保护提出的原因

- 网络与系统最初几乎没有考虑安全，主要关注各种功能实现
- 使用过程中发现：安全问题几乎让**系统设计功能无法完成**
- 网络与系统几乎全是弱点

“提高攻击难度”
就是网络与系统保护的最基本目标。

系统的攻击——以DOS为例

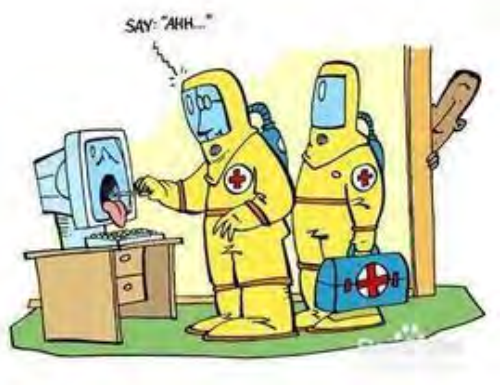
- DOS时代是一个原始社会“**人人平等，个个有权**”
- 应用程序代码可以直接修改中断向量表，可以修改任何系统文件
- 劫持了中断，就可以彻底篡改系统控制流程

系统的攻击——以DOS为例

- DOS时代病毒泛滥
- 中断劫持几乎成了DOS病毒的必选；被病毒劫持了中断的DOS系统就成了病毒的DOS，而非用户的DOS
- 除了中断向量表，引导程序（引导性病毒），可执行程序文件（文件性病毒），都可以被任何应用程序修改；
- 没有安全保护的DOS系统很难确保**系统基本功能的完成；**

系统的保护——直接的对抗

- 病毒查杀工具是DOS时代对抗病毒攻击最主要的技术手段（**风险应对措施**）
  - 病毒查杀工具可以发现病毒篡改系统的痕迹，然后把它修改正确，但是病毒仍然能够继续篡改；
  - 病毒甚至攻击病毒查杀工具；
  - **直接病毒查杀处于一种胶着状态**



系统的保护——信息系统的分级

- 随后的操作系统引入了等级化的概念，计算机系统的等级社会出现了
  - 处理器分为：Ring0-Ring3；
  - 操作系统分为内核和应用层，应用层代码无法修改内核层代码
  - 系统可以运行在内核态和用户态，用户态权利被大大削弱
  - 微软补丁签名，不是微软发布的补丁不能进入Windows系统
  - 计算机对代码的分级管理，阻断了大量的攻击威胁，应用层的攻击蔓延不到内核
  - 计算机系统从“原始社会”进入到了“有等级的文明社会”。

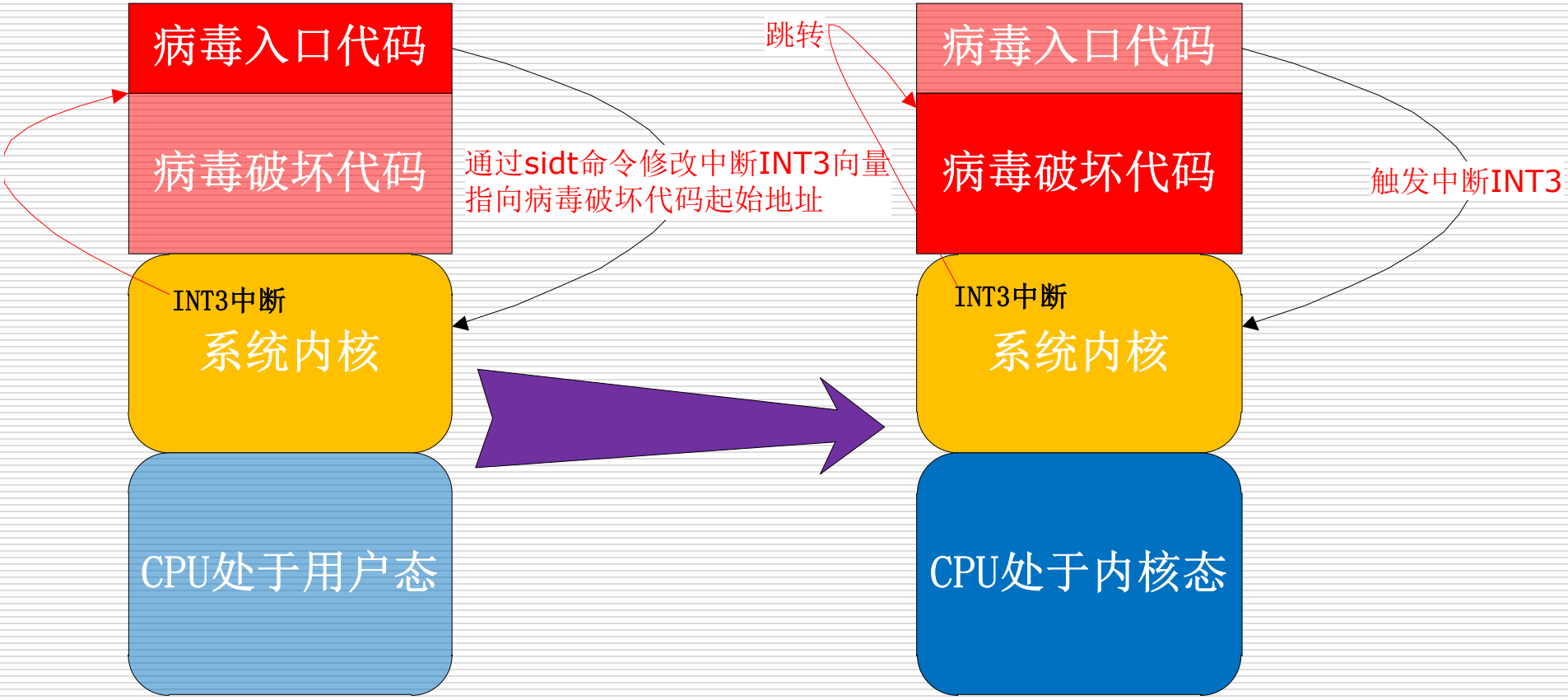
系统的保护——系统分级“规则”在发展

- 系统的“规则”建设工作在不断的发展
  - SELinux（Security Enhanced Linux，安全增强Linux）用MAC（强制访问控制）代替了普通Linux的DAC（自主访问控制）
  - ARM的TrustZone，Intel的TXT（第一代），SGX（第二代）技术，在Ring0-Ring3的基础上进一步细化规则，提供了可信执行环境
  - Android APP Sandbox机制严格隔离了APP权限
  - Android permssion机制限定了APP的行为
  - 系统设计将会越来越复杂

系统的保护——“规则”与弱点

- 法律漏洞不可避免，任何法律都可能存在漏洞
- 信息系统的“规则”也可能存在“漏洞”（本课程将其统一称为“弱点，vulnerabilities”）
  - 系统的“规则”实现依赖代码
  - 大量代码中不可避免的存在弱点
  - 敌手可以利用弱点，绕过“规则”既定的限制，实施破坏

一个系统弱点的例子——CIH病毒



系统的保护——建“规则”和挖“漏洞”

- 系统保护的核心什么？
- 建“规则”
  - “规则”本身的设计是否合理？是否满足技术的发展？《吕氏春秋·察今》“治国无法则乱，守法而弗变则悖”
  - “规则”实施是否完备
- 挖“漏洞”
  - 检验“规则”实施的完备性，是“规则”运转的维护
  - 敌手用来攻击

网络保护

- 网络保护经历了和系统保护类似的过程
  - 最初的TCP/IP协议没有考虑安全问题，仅仅是数据包的高效转发问题；
  - 安全形势的发展使得IPsec和SSL协议成为TCP/IP协议的重要补充；
  - 几乎所有的应用层网络协议都有与之对应的安全协议（HTTPS, DNSSEC）；
  - 安全协议成为IPV6的标配
  - 3G、4G无线通信协议中安全是不可缺少的组成部分

本次课的关键点

- 网络与系统安全的目标
- 网络与系统保护阶段的需求与目标
- **信息系统全生命周安全期阶段的需求与目标**
- 信息系统可生存技术阶段的需求与目标
- 自重构可信赖安全阶段的需求与目标

系统防护技术面临的问题

- 系统防护关注给信息系统中的信息处理过程构建“规则”
- 系统安全保护失效的原因主要包括：
  - “规则”设计的问题：
    - 系统防护的规则是一个不断“精妙化”发展的过程；
    - 所谓“精妙”就是安全好用，但是安全和好用很难同时兼顾；
    - 安全和好用之间一般需要折中，Windows系统使得大部分内核病毒受到控制，但是应用层病毒依然存在；
  - “规则”实施的问题：
    - 保护最终靠软件硬件实现
    - 复杂系统的软硬件实现可能存在不可预知的实现弱点
    - 系统复杂程度越高，实现弱点越多

系统防护技术面临的问题

- 系统安全防护技术追求100%的安全目标难以为继
  - 未来的信息应用场景对规则的设计要求不断提升，例如封闭环境的信息机密性保护，比开放互联中的机密性保护规则设计要更容易一些；
  - 系统安全防护的“成本/效益比”是边际递减的过程，即，前90%的收效需要较小的成本，而后10%的收效则可能需要极高的成本

系统防护技术面临的问题

- 信息技术的发展使得系统不安全、不可控成为常态
  - 信息服务随处可得，背后是即为复杂的信息巨系统和海量的数据产生，弱点发现源源不断；
  - 大量的社会财富聚集网络空间，威胁越来越多，攻击的可能性越来越大；
  - 技术在不断发展，安全的条件在不断变化：云计算、物联网、大数据……
  - 昨天是安全的方案，今天有可能不安全
- **传统系统防护追求100%的安全目标是不合时宜的，所以我们要追求的是适度的安全**

信息安全风险的概念

- 威胁利用弱点破坏信息的安全，即破坏信息的“**CIAA**”特性
- 威胁利用漏洞实施系统安全破坏的过程是一个存在可能性（**LikeHood**）过程；
  - 攻击者能从攻击过程中获得多大利益？漏洞利用的难度？这两项是评价漏洞价值的主要指标
  - 例如，美国不会对一个买日用品的淘宝网店进行APT攻击，如果一个顺手的漏洞，很多人都会尝试一下。

信息安全风险的概念

- 信息安全风险的定义：
  - 威胁（Threats）利用弱点（Vulnerabilities）给信息资产（Assets）造成负面影响（Impacts）的潜在可能（Likelihood）
- 信息安全风险的要素
  - 与威胁和弱点的基本关系相比，信息安全风险又引入了信息资产的概念
  - 信息是有价值的（无价值的信息也有安全属性）
  - 风险取决于可能性和影响
  - 风险三要素包括：威胁、弱点和影响

威胁可能性与信息资产的关系

- 敌手利用弱点进行攻击的可能性取决于：
  - 弱点利用难度；
  - 敌手的获益的多少；
- 一般来说信息资产越大，敌手的获益越大，但不总是这样：
  - 信息资产从保护者的角度来看；
  - 敌手获益从攻击者的角度来看；
  - 因此风险在威胁、弱点基本关系的基础上引入了信息资产的概念

信息安全风险概念下的信息安全目标

- 引入信息安全风险概念后，信息安全的目标将不再是追求100%的安全
  - 保护需要将成本与被保护的信息资产的价值进行对比；
  - 在综合考虑保护成本的基础上追求适度的安全
  - 适度的安全需要对安全风险进行准备的识别和度量
- $\Sigma_{(所有威胁)}$ 信息资产*威胁i*可能性*影响

信息安全目标的总结

- 信息安全的目标本质上是风险控制的过程
- 风险控制的两个显著特点：
  - 1.信息安全目标是一个考虑“成本/收益”的折中结果：
    - 不能追求绝对的安全
    - 只有可以接受的安全
  - 2.信息安全目标的实现是一个动态的无限迭代过程：
    - 环境是不断变化的
    - 控制措施需要相应变化以确保其与风险的适配性

信息安全风险管理

- **信息安全风险管理**：确定威胁利用弱点实施破坏发生的概率（识别风险），决定采取何种措施，将风险降低到**可以接受的水平**。
- **风险管理是一个**“无限迭代”的过程，因为弱点和威胁时时都在变化；
- **风险控制措施**需要在“成本”、“成效”和被保护的“信息资产价值”之间进行**权衡**；
- 很难做到100%的安全，只有折中的安全

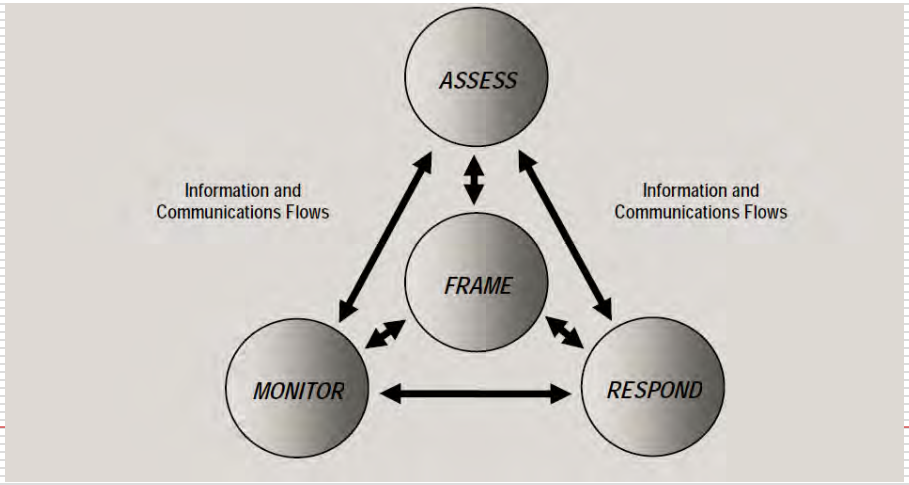
信息安全风险管理的标准流程

- NIST的标准 SP800-39
  - *“Managing Information Security Risk”*
- NIST的标准 SP800-30
  - *“Risk Management Guide for Information Technology Systems”*
- 卡耐基梅隆大学（CMU）的OCTAVE风险评估方法

信息安全风险管理

- 信息安全风险管理的四项工作（NIST SP800-39）
  - 定义风险（安全假定，定义风险），评估风险，风险应对，监视风险
  - 以上过程也是一个典型系统安全论文写作的基本结构；

●安全假定；
●安全分析；
●解决方案；
●未来工作；



风险定义（Framing）

- **风险定义**：完成一个组织如何**评估**、**应对**、**监视**信息系统安全风险的策略性规定，包括
  - 详细的安全假定确定；
  - 安全风险控制实施所受的各种可能的限制；
  - 机构对风险的容忍程度；
  - 风险处理过程中的面临的各种这种决策的优先次序。

PS：机构是一个信息安全的责任实体，可能是一个企业，也可能是一个事业单位。

风险评估（Assessing）

- **风险评估**：确定机构**运行**、**资产**和**个人**可能遭受的风险，并对风险进行量化评估和排序
  - 机构运行包括：机构业务，机构职能、机构声誉等内容；
  - 风险评估依据由**漏洞、威胁引发的攻击的概率**以及攻击对机构运行，资产和个人的影响进行量化评估；
  - 根据风险量化结果进行风险优先排序

PS：所以在漏洞分析研究中，除了漏洞的数量，漏洞的影响，以及漏洞利用的难易程度都是需要考虑的重要衡量指标。

风险应对（Responding）

- **风险应对**：评估、确定采取何种措施来**接受，规避，消减**甚至是**转移**机构运行、资产和个人面临的信息安全风险；
  - 输出是：“采取何种措施”，即信息安全控制措施；
  - 风险应对有一个灵活的目标，其成效包括：接受、规避、消减和转移风险，而不是简单的消灭风险；

PS:风险应对措施就是我们采取的安全保护措施，安全保护措施的目标直接决定安全保护措施的具体实施方案

风险监视（Monitoring）

- **风险监视**：使机构具备了解风险应对措施的适配性和改进风险应对措施的能力，主要工作包括：
  - 确认风险应对措施是否安全既定设计实施（*compliance*）；
  - 检查风险应对措施的实际应用效果（*effectiveness*）；
  - 发现能够影响信息系统风险的系统和运行环境的变化，并作出反映；

PS：信息安全风险管理成为一个无限次的迭代过程；

全生命周期安全

- 基于时间的PDR模型
  - PDR的基本含义：P防护protection；D检测detection；D响应response
  - Winn Schwartau于1998年提出。书籍为《Time Based Security》
  - PDR经过发展，延伸出来各种版本
  - **PDR伴随信息系统运行的整个生命周期**
  - PDR推动了入侵检测系统（Intrusion Detection System，IDS）的发展
  - PDR模型属于技术范畴

全生命周期安全——基于时间的安全

基于时间的安全

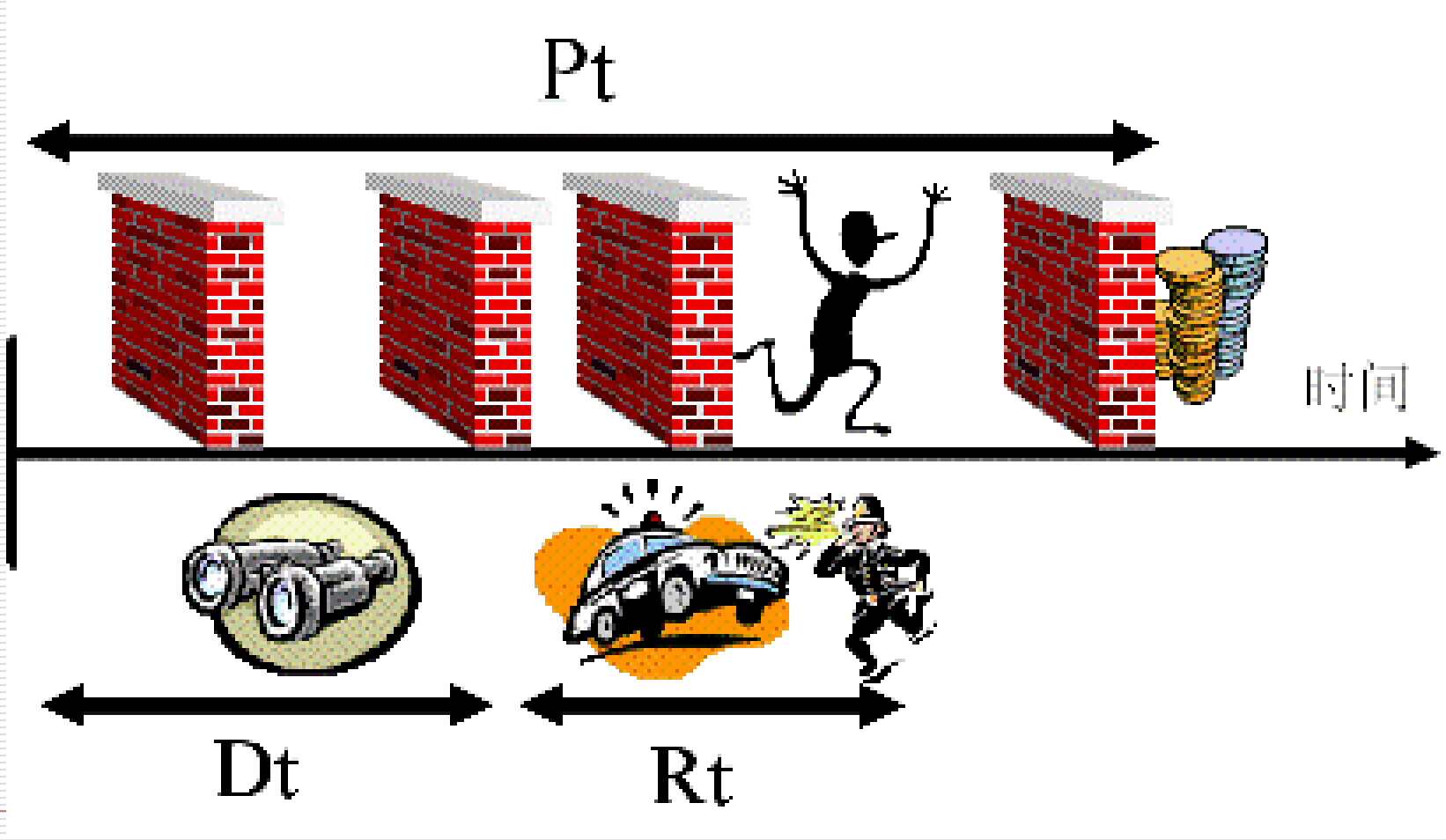
- 以时间为度量指标，量化描述系统攻击和防御的对抗，著名的安全条件如下：

$$Pt > Dt + Rt$$

其中：

- Pt：是因为系统保护的实施，使得敌手攻击要花费的时间，Pt越大表明敌手攻击需要的时间越长，系统防护越有效，例如分组密码抵抗攻击的轮数，密钥的长度等
- Dt：检测、发现攻击的时间，例如入侵检测，和当下的攻击预警系统，Dt要越小越好
- Rt：应对一个攻击的时间，最直接的例子就是蠕虫攻击中的打补丁时间，Rt越小，说明系统安全反应越灵敏

全生命周期安全——基于时间的安全



全生命周期安全——信息安全管理

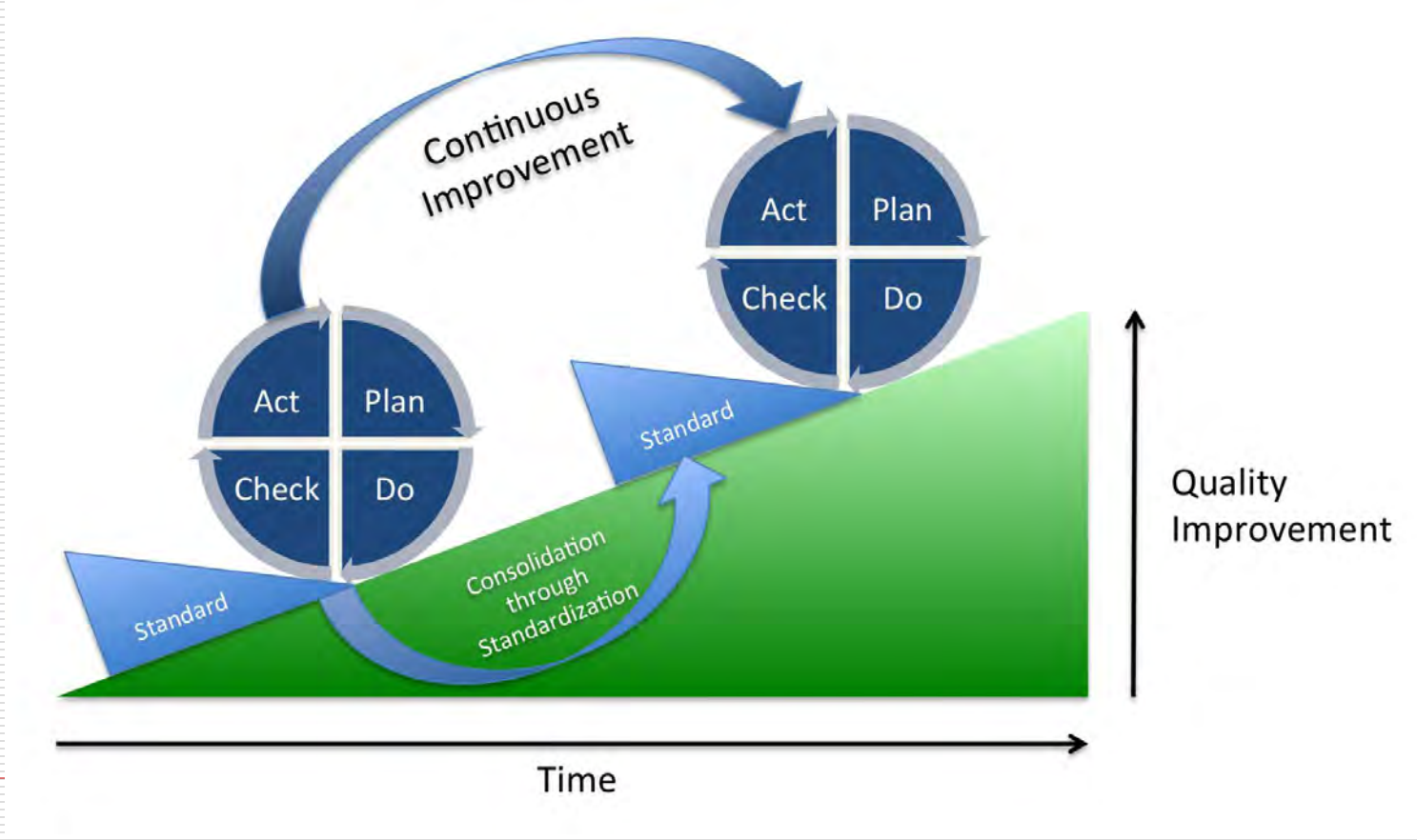
- 在技术手段之上，采用管理的手段，对信息系统进行全生命周期
- 管理措施贯穿信息系统的设计、实施、运行等整个生命周期
- 相关的标准：
  - ISO/IEC 27001
  - BS7799
- 提出了著名的信息安全管理：ISMS PDCA模型

全生命周期安全——PDCA

- PDCA：Plan-Do-Check-Act
  - Plan：对ISMS范围所及进行风险评估和控制方案设计
  - Do：对于不可接受风险，实施风险处理计划，比如增加防火墙等安全措施；
  - Check：分析运行效果，寻求改进机会，国际上所有管理类标准都有该持续改进的环节，比如著名的ISO9001
  - Act：经过了评审之后，要执行的进一步动作

全生命周期安全——PDCA

- PDCA是一个不断循环的过程



全生命周期安全——入侵检测IDS

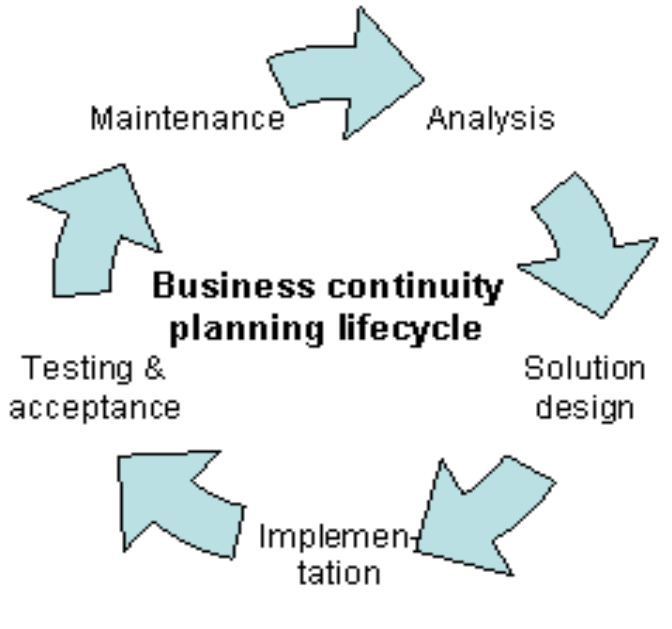
- IDS是PDR模型的中的重要支撑技术
- IDS主要的功能为：监视、评估信息网络系统中的恶意或者违反安全策略的行为，并产生相应的报警
- IDS伴随信息系统的运行工作，构成了系统“规则”之后的第二道防线；
- IDS的核心概念为：**报警及报警的误报率和漏报率**
- IDS与防火墙和防病毒软件合称为信息安全的“老三样”

全生命周期安全——灾难备份与恢复

- 及时构建了系统安全机制，配备了IDS系统，信息系统还存在可能发生自然或者认为的灾难
- 信息系统需要制定计划应对这些灾难的发生
- 信息安全管理标准BS7700中提出了业务连续性（Business Continuity Plan，BCP）的重要性，2006年英国国家标准组织BSI，发布了BCP指导标准BS 25999-1

全生命周期安全——灾难备份与恢复

- BCP关键支撑技术为数据灾备技术



课程提纲

- 网络与系统安全的目标
- 网络与系统保护阶段的需求与目标
- 信息系统全生命周期安全阶段的需求与目标
- 信息系统生存技术阶段的需求与目标
- 自重构可信赖安全阶段的需求与目标

全生命周期安全技术面临的问题

- 系统保护机制的弱点使得对系统攻击成功的概率一直存在
- 全生命周期的PDR技术虽然提供了对攻击的预警和应对机制，但是可以从基于时间的安全不等式看出，安全的条件不能总是满足，Pt<Dt+Rt的情况时有发生
- 信息系统需要在全生命周期保护的基础上增加新的保护
- **如果系统在遭受“*特定程度*”的攻击时仍能够正确运行，系统的安全性将大为增加**

信息系统生存技术——可靠计算和错误容忍

- 信息系统生存技术关注：**信息系统通过特定的设计，变得不是那么脆弱，一碰就倒，一触即溃。**
  - 一个普通玻璃盘子是fragile的很容易摔碎，康宁公司通过特殊设计使得盘子即使被摔也不会被摔碎
  - 信息系统生存技术，通过技术设计，比如虚拟机迁移，一个硬件故障，可以迅速迁移到另一台硬件设备，继续运行
  - 信息系统生存技术关注：计算过程的可靠性和错误容忍

信息系统生存技术——可靠计算和错误容忍学术组织

- 国际著名的可靠计算和错误容忍
  - **The IEEE Technical Committee on Dependable Computing and Fault Tolerance**
  - **IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance**
- **IEEE/IFIP**共同举办了**旗舰会议：The IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)**讨论可靠计算和入侵容忍每年的技术发展。

信息系统生存技术——区别*错误容忍*和*灾难恢复*

- 系统生存技术和灾难恢复都用到数据和系统备份技术，并关注信息系统业务功能运行连续性。
- 错误容忍是系统内在的安全设计，在一定程度的攻击或者局部失效的情况下，系统仍然能够正确运行，冗余备份是系统生存设计的一种形式，但是不限于该形式
- 灾难恢复关注在发生自然或者人为信息系统灾难时，仍然能够通过备份的数据或者系统快速恢复业务
- **就像一个人，**
  - **感冒仍能够工作属于可生存技术范畴，**
  - **事故截肢，再装假肢工作属于据灾难恢复范畴**

信息系统生存技术——系统生存技术特点

- 系统生存技术关注消除系统的单点失效，系统分布在多个点上，通过机制设计使得少数几个点的错误不会导致系统失效
- 系统生存技术可以容忍个别点的背叛，而不仅仅是失效，因此，生存技术不仅可以抵御外部攻击，还可以抵御内部背叛
- 系统生存技术关注**权力集中的消除**

信息系统生存技术——分类

- 实现入侵容忍有两种途径。
  - 第一种途径是攻击响应，通过改进检测系统，加快反应时间，从而将信息保障技术上升到一种在攻击发生的情况下能够继续工作的系统。
    - 该途径直接继承和发展了信息保障技术
  - 第二种则被称为攻击遮蔽，攻击发生了以后，整个系统好像没什么感觉。
    - 系统入侵容忍具体技术包括拜占庭容错技术、门限密码技术等

信息系统生存技术——拜占庭将军问题

- 拜占庭将军问题是容错计算中的一个老问题，1982年由Lamport, Shostak, Pease提出
  - 邦占庭帝国是5～15世纪的东罗马帝国。几支部队包围着敌人的一座城市。每支部队都由它自己的将军统帅。统帅之间只能通过报信者互相通信。他们必须统一行动。
  - 某一位或几位统帅可能是叛徒，企图破坏忠诚的司令们的统一行动。
  - 将军们必须有一个算法，使所有忠诚的将军能够达成一致，而且少数几个叛徒不能使忠诚的将军们做出错误的计划。

信息系统生存技术——拜占庭将军问题

- Lamport证明了：有m 个叛国统帅，则统帅们的总数必须为3m+1 个以上，才能确保消息协商的正确性
- 以此类推，有3m+1个组件组成的系统可以容忍m组件的背叛（损坏，被敌手控制）
- **拜占庭将军问题量化了系统备份对系统安全的促进效果**

信息系统生存技术——门限密码

- 1979年Shamir提出密码分享后，Desmedt等人于1994年正式提出了门限密码学的概念
- 拉格朗日差值定理确定：n个不同点可以确定n-1次多项式。多项式上任何n个不同点都可以确定确定同一个多项式
  - 比如，可以将一个二次多项式的常数项作为重要事务的处理密钥，将二次多项式上5个不同的点信息分发给5个主管领导，则任何3个领导到场都可以恢复出事务处理密钥，完成事务，避免单点失效

课程提纲

- 网络与系统安全的目标的需求与目标
- 网络与系统保护阶段的需求与目标
- 信息系统全生命周安全期阶段的需求与目标
- 信息系统生存技术阶段的需求与目标
- 自重构可信赖安全阶段的需求与目标

生存技术面临的问题

- 生存技术通过分散系统的安全依赖获得对系统错误的容忍
- 一定数量的可信可控系统存在是生存技术发挥作用的前提
- 信息技术的发展改变了生存技术的安全假定
  - 信息处理的社会化分工，和信息服务的高度灵活可获取性，使得一定数量的可信可控系统的存在变得较为困难
  - 攻击手段的提升使得，静态的被动防御的成本/收益边界递减更为明显

自重构可信赖技术——改变"博弈规则"技术

- 信息安全攻击和防御本质上是一种博弈
- 部署一个信息系统，添加保护措施，进行全生命周期的PDR（检测防御），通过设计增加系统的入侵容忍能力
- 但是信息系统及其安全措施都在哪里，威胁处于主动地位，可以根据自己的情况，选择何时，以何种形势发起攻击
- “敌暗我明”的阵地防御是信息安全防御处于不利地位
- 最新的信息安全技术需要改变这种博弈规则

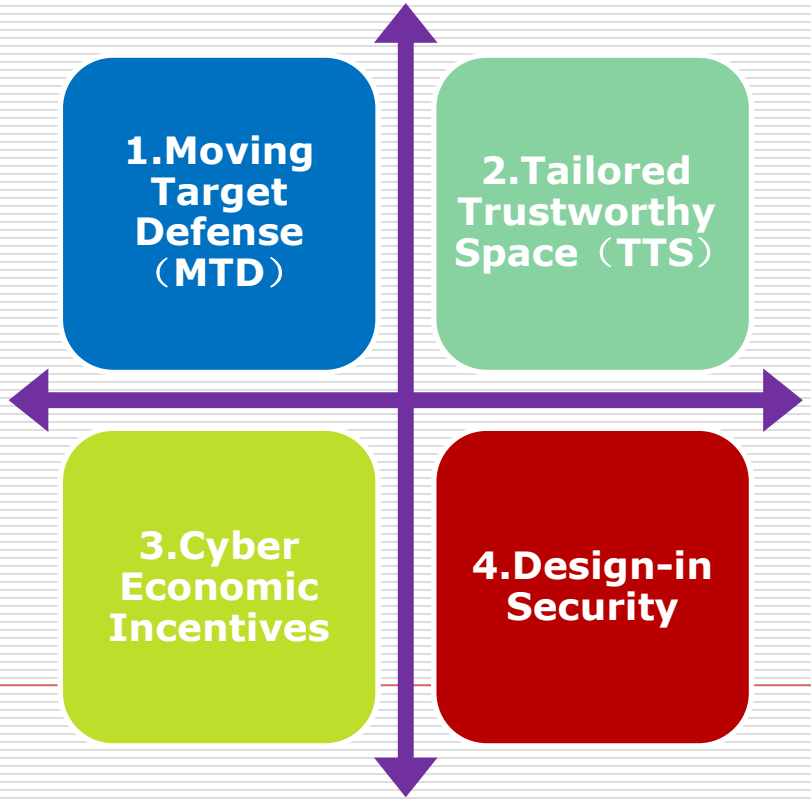
自重构可信赖技术——改变"博弈规则"技术

- **“善攻者，敌不知其所守。善守者，敌不知其所攻”——《孙子兵法.虚实篇》**
  - 善于进攻者与善于防御者在战争中都能掌握主动权。前者往往采取声东击西的手段来迷惑敌人，让敌人摸不清虚实，然后才找到破绽，歼灭敌人。同理，善守防御的人，通过虚虚实实的手段，使攻者不知道自己的底细，不知道从什么地方进攻好。

自重构可信赖技术——

美国“Game Change”的安全技术研究计划

- 美国NITRD制定和正在实施“Game Change”的信息安全技术研究计划，是其国家战略



自重构可信赖技术——

Moving Target

- 愿景**Vision**
  - 系统的功能和服务，由多样化的、不断切换的、随时间变化的机制和策略来实现
- 解读
  - 每一种机制和策略，都可能存在漏洞和被攻击
  - 攻击者必需在切换变化之前，有限时间内完成全部攻击
    - 否则，在切换变化之后，要重新开始
    - 不同于传统的故障恢复；**MT**切换之后是进入不同的机制和策略
  - 射击运动的活动靶
    - 必须在有限时间内、迅速完成射击并命中
    - 否则靶就飞走了

自重构可信赖技术——

Tailored Trustworthy Space

- 愿景**Vision**
  - 灵活的、自适应的、分布式的可信环境，支持多种不同活动的功能和策略要求；包括：
    - 机密性、匿名、数据和系统完整性、起源、可用性和性能
- 解读
  - 当用户执行某活动时，能有效组合网际空间中的设备、措施和方法，形成“满足用户活动的安全需求”的安全环境
    - 协商、调用和整合分布式环境中的安全能力
  - 订制：不同用户活动，对应不同安全属性、有不同的保障级别

自重构可信赖技术——

Cyber Economic Incentives

- 愿景**Vision**
  - 发挥经济学在网际安全中的激励作用
    - 相关的市场、决策和动机的科学理解
  - 推动形成如下的环境
    - 安全技术部署是均衡协调的
    - 提供激励以促进有益的网际行为、阻止有害的网际行为
- 解读
  - 通过经济激励，推动安全技术的实施、有益的行为
    - 目前有很多攻击已有有效的防御措施。但是，没有广泛地部署
  - 网际经济学的前提：相应的统计数据和经济学模型

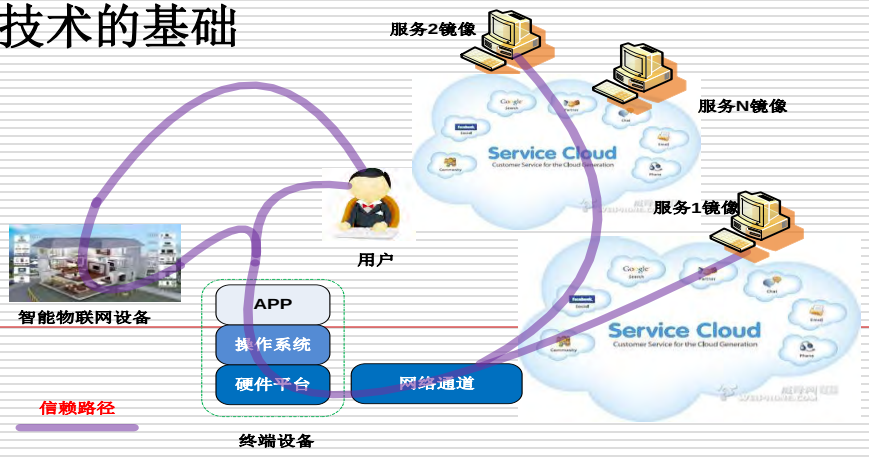
自重构可信赖技术——

Design-in Security

- 愿景**Vision**
  - 采用关注安全的方法、语言和工具，进行系统开发，在具备系统功能的同时，产生安全保证
- 解读
  - 在信息系统功能设计时，将安全功能作为其必选功能进行系统设计，安全功能与系统功能密切结合，避免后续添加安全功能实现可能面临的不足

自重构可信赖技术

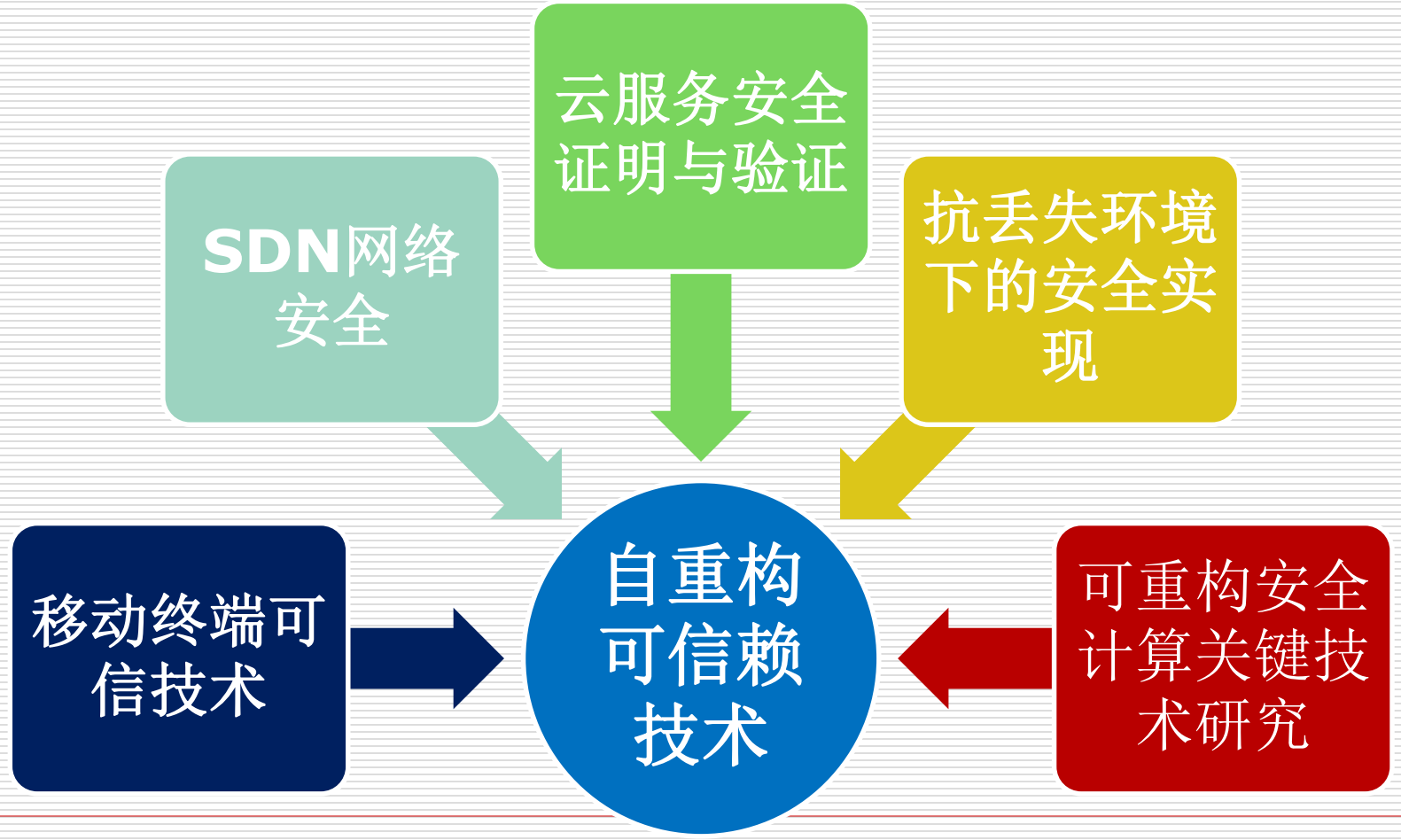
- 信息系统越来越复杂，全面的系统防护变得非常困难。网络规模越来越大，结构越来越复杂，全面的网络保护和监管难以为继
- 甲的可信网络不再是乙的可信网络
- 可重构信赖技术（动态建立，程度范围可证明）
  - 在复杂的网络环境中，根据应用需求，在规模、粒度、位置、时间和信赖程度等多个方面按照安全要求动态地建立起可以被证明的适度可信赖的路径和子网络。
  - 终端的灵活可信建立技术，虚拟网络可定义技术以及服务可信证明技术等是该技术的基础



自重构可信赖技术

- 自重构可信赖技术本质上是：对系统保护弱点的隐藏
  - 保护系统动态生成、动态消失，敌手没有足够的时间获得保护系统的弱点；
  - 保护系统针对应用定制保护，不同的保护存在不同的弱点，保护的异构性增加了敌手获得弱点的难度
  - 有针对性的保护简化了系统降低了弱点的数量

自重构可信赖技术


云服务安全证明与验证
SDN网络安全
抗丢失环境下的安全实现
移动终端可信技术
自重构可信赖技术
可重构安全计算关键技术研究

自重构可信赖技术的支撑技术

- Intel的SGI（TXT）技术，SGX技术
- AMD的SVN 技术
- ARM的TrustZone技术
- Intel Atom 的可信保护技术
- 卡内基梅隆大学（CMU）的Flicker系统
- TCG的TPM2.0和MTM2.0

思考题

- 弱点和威胁的区别？
- 为什么会引入信息安全风险管理？
- 信息安全技术发展的四个阶段内在动力是什么？
- 网络与信息安全的基本需求是那四项？
- 四项安全需求的保护方式是什么？

参考文献

- 1.NIST的标准 SP800-39
  - Managing Information Security Risk
- 2.NIST的标准 SP800-30
  - Risk Management Guide for Information Technology Systems
- 3.OCTAVE风险评估方法
- 4. Time Based Security http://www.amazon.com/Time-Based-Security-Winn-Schwartau/dp/0962870048