浙江大学电气工程学院
College of Electrical Engineering Zhejiang University

# 网络安全导论

## 概述、基础知识

1. **概述、基础知识**
2. 加密与认证技术
3. 软件与通讯安全
4. 电力工控系统安全
5. 物联网终端安全
6. 智能无人系统安全

# 课程介绍

## ❖课程概述

- **课程名称**：《网络安全导论》
- **授课形式**：讲座 + 汇报
- **预修要求**：了解计算机技术、控制理论、电气工程的专业基本知识。

## ❖学习资料

- Handbook on Securing Cyber-Physical Critical Infrastructure, Das, Sajal K. et al, Elsevier, 2015.
- 《网络空间安全导论》，电子工业出版社
- 《物联网安全》，高等教育出版社
- 重要网络安全学术会议论文、期刊论文
- 慕课、公开课资源
- ……

# 课程介绍

- 潘锴锴，特聘研究员、博导
- 浙江大学电气工程学院，智能系统安全实验室（USSLAB）
- 博士/博士后：荷兰代尔夫特理工大学
- 研究方向：新能源安全、控制安全、无人系统安全
- 个人主页：https://person.zju.edu.cn/pkk
- 邮箱：pankaikai@zju.edu.cn
- 地点：教二325，欢迎前来讨论问题！

# 课程介绍

## ❖课程信息：

- 课程主页：学在浙大
- 课程助教：钟启迪，
  12310095@zju.edu.cn
  汪锐
  rayw@zju.edu.cn
- 课程钉钉群

## ❖成绩组成：

- 课堂表现（10%）
  - 出勤、课堂讨论、展示&提问
- 课程展示（50%）
  - 专题调研、PPT汇报
- 课程作业（40%）
  - 课程展示内容复现并提交报告

# 课程目标

## 内容目标

- 掌握网络安全基本知识。
- 网络安全新威胁研究：物联网终端安全、电力工控系统安全、智能无人系统安全。
- **对某一专题深入了解领域前沿。**

## 能力目标

- **专业能力**：了解网络安全威胁来源，利用所学知识进行安全问题分析等。
- **通用能力**：提升个人学习能力、发现与分析问题能力、发散思维能力等。

**通过一门课，入门一个领域。**

## 思政目标

- 领会习总书记对国家关键基础设施安全的重要指示。
- 提升投入国家网络安全“新战场”的热情与动力。
- 领悟功能实现与安全隐患间可能存在的辩证关系。

# 课程要点

- 网络安全威胁事件
- 网络安全的发展与演变
- 网络安全内涵 （“是什么”）
- 网络安全体系结构 （“是什么”）
- 网络安全模型 （“做什么”）
- 网络安全防御策略/原则 （“怎么做”）
- 网络安全保障技术框架、实例

# 网络安全威胁

半个美国网络瘫痪因遭受攻击 Mirai病毒感染

2016-10-22 18:00 出处 综合

半个美国网络攻击事件

网易汽车 网易首页 应用 网易考拉 LOFTER

网易首页 > 汽车频道 > 行业动态 > 正文

国内发生特斯拉第一起自动驾驶事故

2016-08-05 11:21:06

本页位置：首页 → 新闻中心 → 国际新闻 国际频道：

因遭"震网"病毒袭击 伊朗核电站恐发生泄露事故

2011年02月01日 10:00 来源：人民网 参与互动(0) 【字体：↑大 ↓小】

**我们生活的世界还安全吗**

# 网络安全威胁

## Mirai病毒攻击事件（物联网病毒鼻祖）

2016年10月21日发生一系列 DDoS攻击，美国大批知名的国际网站遭到网络攻击，导致主要互联网平台和服务无法使用。

WORLD
2016.10
社会安全

事件影响

尽管它的最初的创造者已经被抓住，他们的源代码仍然存在。它产生了诸如Okiru、Satori、Masuta和PureMasuta等变体。例如，PureMasuta能够将D-Link设备中的HNAP漏洞武装化。

类似事件

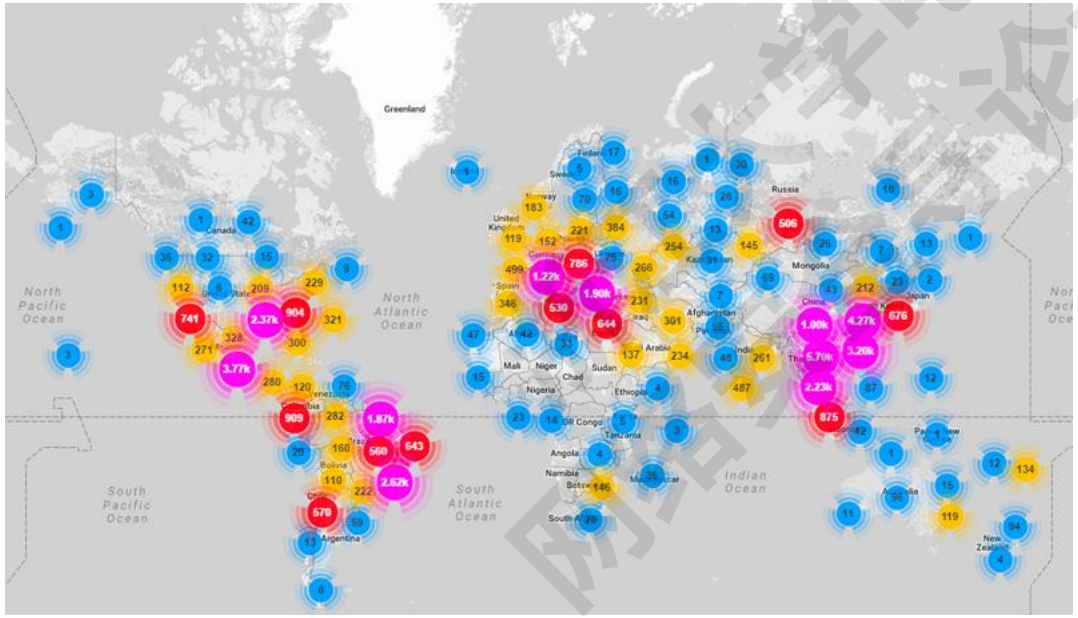
截至十一月2016年底，大约900 000项路由器，从德国电信和智易产生，是由于失败的TR-064开发试图通过未来的变体，导致这些设备的用户在互联网连接问题坠毁。

- Airbnb[11]
- Amazon.com[8]
- Ancestry.com[12][13]
- *The A.V. Club*[14]
- BBC[13]
- *The Boston Globe*[11]
- Box[15]
- *Business Insider*[13]
- CNN[13]
- Comcast[16]
- CrunchBase[13]
- DirecTV[13]
- *The Elder Scrolls Online*[13][17]
- Electronic Arts[16]
- Etsy[11][18]
- FiveThirtyEight[13]
- Fox News[19]
- *The Guardian*[19]
- GitHub[11][16]
- Grubhub[20]
- HBO[13]
- Heroku[21]
- HostGator[13]
- iHeartRadio[12][22]
- Imgur[23]
- Indiegogo[12]
- Mashable[24]
- National Hockey League[13]
- Netflix[13][19]
- *The New York Times*[11][16]
- Overstock.com[13]
- PayPal[18]
- Pinterest[16][18]
- Pixlr[13]
- PlayStation Network[16]
- Qualtrics[12]
- Quora[13]
- Reddit[12][16][18]
- Roblox[25]
- Ruby Lane[13]
- *RuneScape*[12]
- SaneBox[21]
- Seamless[23]
- *Second Life*[26]
- Shopify[11]
- Slack[23]
- SoundCloud[11][18]
- Squarespace[13]
- Spotify[12][16][18]
- Starbucks[12][22]
- Storify[15]
- Swedish Civil Contingencies Agency[27]
- Swedish Government[27]
- Tumblr[12][16]
- Twilio[12][13]
- Twitter[11][12][16][18]
- Verizon Communications[16]
- Visa[28]
- Vox Media[29]
- Walgreens[13]
- *The Wall Street Journal*[19]
- Wikia[12]
- *Wired*[15]
- Wix.com[30]
- WWE Network[31]
- Xbox Live[32]
- Yammer[23]
- Yelp[13]
- Zillow[13]

# 网络安全威胁

## Mirai病毒攻击事件　　攻击影响范围

- 下图为Mirai感染的设备位置分布图
- 右表为Mirai DDoS攻击起源的主要国家




| Country | % of Mirai botnet IPs |
|---|---|
| Vietnam | 12.8% |
| Brazil | 11.8% |
| United States | 10.9% |
| China | 8.8% |
| Mexico | 8.4% |
| South Korea | 6.2% |
| Taiwan | 4.9% |
| Russia | 4.0% |
| Romania | 2.3% |
| Colombia | 1.5% |

# 网络安全威胁

## “震网” – 伊朗核电站事件

Stuxnet蠕虫（俗称“震网”）在2010年7月开始爆发,攻击目标包括核电站、水坝水利设施、国家电网等。伊朗政府已经确认该国的布什尔核电站遭到Stuxnet蠕虫的攻击，导致铀浓缩离心机受损。（第一个攻击基础设施）

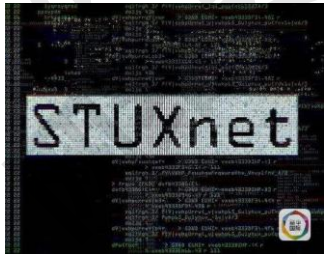
IRAN
2010.07
国防安全

**原因分析**

它利用了微软操作系统中至少4个漏洞，其中有3个全新的零日漏洞；它是第一个直接破坏现实世界中工业基础设施的恶意代码。

**类似事件**

火焰病毒是一种2012年5月被发现的计算机病毒，大约从2010年开始散播，在中东大范围传播，涉及伊朗、以色列、巴勒斯坦，以及叙利亚、黎巴嫩、沙特等国家。




# 网络安全威胁

## BlackEnergy – 乌克兰停电事件

**2015年12月23日，乌克兰电力部门遭受到恶意代码攻击，Kyivoblenergo电力公司发布公告称7个110KV的变电站和23个35KV的变电站出现故障，导致80000用户断电。（第一个黑客攻击导致的电网停电事件）**

Ukraine
2015.12
关基安全

原因分析

这次事件以BlackEnergy等相关恶意代码为主要攻击工具，结合多种攻击手段，最后造成长时间停电和整个社会的混乱。

类似事件

2016年1月15日，根据CERT-UA的消息，乌克兰最大机场基辅鲍里斯波尔机场网络遭受BlackEnergy攻击。


# 网络安全威胁

## BlackEnergy – 乌克兰停电事件

# 网络安全威胁

智能摄像头

智能光伏逆变器

智能照明设备

智能路由器

智能门锁

智能音箱

智能汽车

智能洗衣机


智能电视

智能空调

智能冰箱

智能热水器

# 网络安全威胁

隐私偷窥

新能源攻击

恶意闪烁

恶意流量收集

门禁形同虚设

窃听设备

驾驶安全

大规模需求攻击


隐私窥探

恶意加热/制冷

挖矿设备

大规模需求攻击

# 网络安全威胁

从日常生活的手机、电脑、智能家居，到医疗、电力、国防安全，这些事件报道说明，我们的生活并不安全。随着人工智能、新一代通信、物联网等的发展，**信息世界与物理世界**跨域融合，网络安全**威胁来源**和**危害**愈发复杂，威胁着我们的**隐私**、**财产**安全，甚至是**生命**安全。网络安全的**内涵**和**外延**已经发生深刻变化。

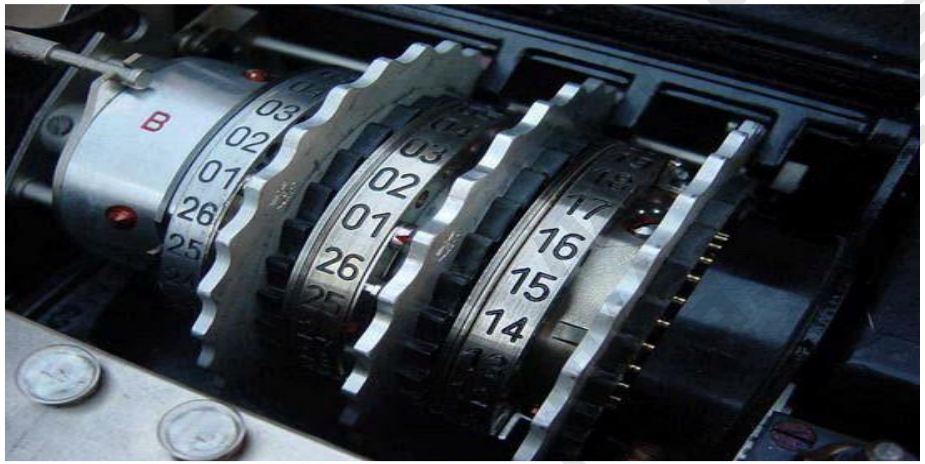
“现状：很酷的新兴技术在一阵匆忙中被实施，系统的安全性通常在出现问题后才被想起。”---Steve Jobs

“网络世界必然存在安全问题（伴生性）”。

# 网络安全的发展与演变

## ❖通信安全时代

- 通信安全（COMSEC）时代：19世纪70年代前，重点是通过密码技术解决通信保密问题，主要安全威胁是搭线窃听和密码分析，采用的保障措施就是加密，确保**机密性**和**完整性**。
- 其时代**标志**是1949年Shannon发表的《保密通信的信息理论》和1977年美国国家标准局公布的数据加密标准（DES）。



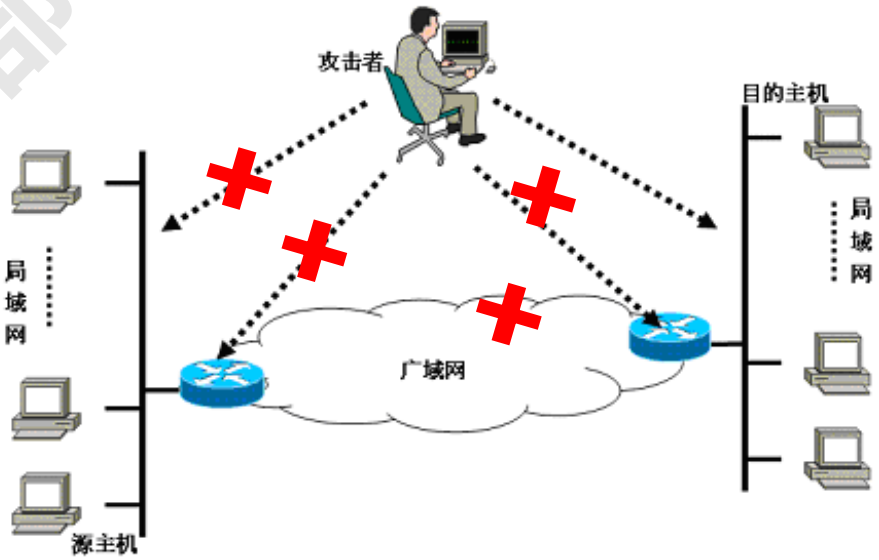
“恩格玛”密码机


二战和朝鲜战争中美国的密码装备（M-209）

# 网络安全的发展与演变

## ❖信息/网络安全时代

- **重点**是确保计算机和网络的硬件、软件，所存储、处理和传输的信息的安全。**主要安全威胁**是非法访问、恶意代码、网络入侵、病毒破坏等。
- **主要保障措施**是安全通信协议、安全操作系统(TCB)，以及防火墙、防病毒软件、漏洞扫描、入侵检测、PKI、VPN和安全管理等安全技术。
- 其时代**标志**是1985美国国防部公布的可信计算机系统评价准则（TCSEC）和ISO的安全评估准则CC（ISO 15408）。



# 网络安全的发展与演变

## ❖信息/网络安全 --- TCSEC安全级别

| 类别 | 级别 | 名称 | 主要特征 |
| --- | --- | --- | --- |
| D | D | 低级保护 | 没有安全保护 |
| C | C1 | 自主安全保护 | 自主访问控制 |
| | C2 | 受控访问控制 | 单独的可查性，安全标识 |
| B | B1 | 标识的安全保护 | 强制访问控制，安全标识 |
| | B2 | 结构化保护 | 面向安全的体系结构，较好的抗渗透能力 |
| | B3 | 安全区域 | 访问控制，高抗渗透能力 |
| A | A | 验证设计 | 形式化的最高级别描述和验证 |

# 网络安全的发展与演变

## ❖信息/网络安全保障时代

- 保证信息和信息系统的**保密性、完整性、可用性、可控性、真实性和不可否认性**的信息安全保护和防御过程。它要求**加强**对信息和信息系统的保护，**加强**对信息安全事件和各种脆弱性的检测，**提高**应急响应能力和系统恢复能力。

# 网络安全的发展与演变

## ❖信息/网络安全保障时代

**作用领域**

- 网络空间
- 物理空间
- 电磁空间

**防护技术**

- 密码加密
- 身份认证
- 等级保护
- 监测预警
- 应急响应
- 容错备份
- 风险评估

# 网络安全的发展与演变

## ❖信息/网络安全保障时代

- **网络**


**欧洲**：能源巨头EDP公司芯片被破解遭恶意攻击

**印度**：泰米尔纳德邦核电站内网后台感染恶意软件

**法国**：后门攻击导致费森海姆核电站敏感数据泄露

**美国**：俄罗斯黑客攻击美国核电站和供水设施

**伊朗**：震网病毒攻击PLC，破坏核设施


**乌克兰**：黑色能量病毒攻击电闸，大面积停电

- **物理**


**罗马尼亚**：ING数据中心受声音影响，宕机10小时

**美国**：无人机攻击宾夕法尼亚州的变电站，造成数百万美元损失

**委内瑞拉**：电磁攻击，大面积停电

# 网络安全的发展与演变

## ❖信息/网络安全的时代特征

### （1）安全危害的倍增性

- 现代网络牵一发而动全身，基础设施越“智能”，对网络的依赖程度越高，受攻击的可能性就越大。
- 一旦遭受攻击，危害范围会由区域向广域扩散，由个体向群体蔓延，由一种危害引发多种危害。
- 具有典型的“蝴蝶效应”，危害程度会呈非线性激增，可使被攻击者瞬间成为“瞎子”、“聋子”、“瘫子”。

# 网络安全的发展与演变

## ❖信息/网络安全的时代特征

### （2）安全对抗的非对称性

- 按照“木桶原理”，网络安全防御水平取决于最薄弱的环节，攻击者只要突破防御体系中的一个缺口，就有可能导致整个防线崩溃。
- 与传统对抗相比，防御需要全面设防，攻击只需攻其一点，难守而易攻。

# 网络安全的发展与演变

## ❖信息/网络安全的时代特征

### （3）安全发展的动态性

- 网络安全是一个不断发展的过程，攻击技术层出不穷，安全技术必须与时俱进。
- 面对网络安全威胁技术与手段的不断更新，要求网络安全保障工作必须及时调整安全策略，提高“风险检测 - 实时响应 - 策略调整 - 风险降低”的自适应能力，在动态中确保有效防护。
- “不存在一劳永逸确保安全的技术和方法。”

# 网络安全内涵

## ❖国际标准化组织（ISO）定义：

- 在技术上和管理上为数据处理系统建立的安全保护，保护**计算机硬件、软件和数据**不因偶然和恶意的原因而遭到**破坏（可用性）、更改（完整性）和泄露（保密性）**。

- ISO标准17799：2005

ISO: International Organizations for Standardization

# 网络安全内涵

## ❖网络安全基本属性

**三个基本属性**

- **保密性（Confidentiality）**
- **完整性（Integrity）**
- **可用性（Availability）**

**其他属性**

- **可控性** 指授权实体可以控制信息系统和信息的使用
- **不可否认性** 对出现的安全纠纷可提供调查依据和手段

# 网络安全内涵

## ❖保密性

保密性(confidentiality)是指网络信息不被泄露给非授权的用户、实体或过程。

常用的**保密技术**包括：

- **物理保密**：利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露。
- **防窃听**：使对手监收不到有用的信息。常用的防窃听技术包括电磁干扰、超声波干扰等。
- **防辐射**：防止有用信息以各种途径辐射出去。
- **信息加密**：在密钥的控制下，用加密算法对信息进行加密处理。

# 网络安全内涵

## ❖完整性

完整性（integrity）是指网络信息在未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

### 区别

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求**信息不致受到各种原因的破坏。**

### 影响因素

设备故障、误码(传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码)、人为攻击、计算机病毒等。

# 网络安全内涵

## ❖完整性

保障网络信息完整性的**主要方法**有：

**协议**：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段;

**纠错编码方法**：由此完成检错和纠错功能。最简单和常用的纠错编码方法是奇偶校验法。

**密码校验和方法**：抗篡改和传输失败的重要手段;（同样作用于机密性）

**数字签名**：保障信息的真实性;

**公证**：请求网络管理或中介机构证明信息的真实性。

# 网络安全内涵

## ❖可用性

可用性是网络信息可被授权实体访问并按需求使用的特性。网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

保障网络信息可用性的**主要方法**有：

**身份识别与确认、访问控制**：对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。

**路由控制**：选择稳定可靠的子网，中继线或链路等。（同样作用于机密性）

**审计跟踪**：把网络信息系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便分析原因，分清责任，及时采取相应的措施。

# 网络安全内涵

## ❖网络空间安全（Cyberspace Security）

- 网络空间安全是能够用来保护**网络空间环境与组织和用户资产**的工具、策略、安全概念、安全防护措施、指南、风险管理方法、行动、培训、最佳实践、保障的集合。
- 组织和用户资产包括连接的**计算设备、个人信息、基础设施、应用、服务、电信系统以及所有的传输和/或存储在网络空间环境中的信息**。
- ITU T X.1205 建议书《 网络安全综述 》： 2008

网络空间安全涵盖了传统的信息/网络安全的内容，但其侧重点是与陆、海、空、太空等并行的空间概念，反映的安全问题**具有跨时空、多层次、立体化、广渗透、深融合的新形态。**

# 网络安全内涵

## 网络安全内涵的通俗说法…

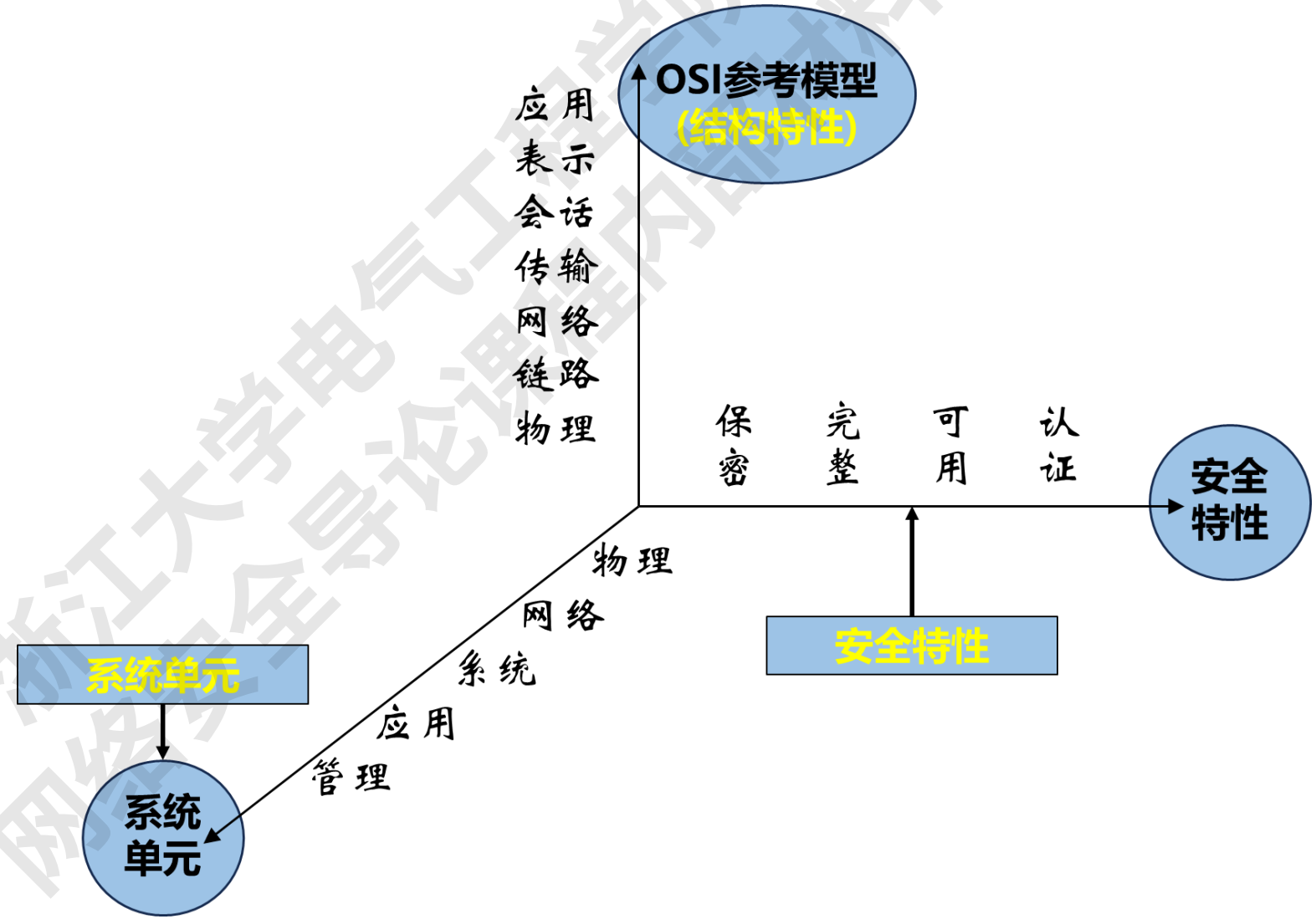
- 进不来
- 拿不走
- 看不懂
- 改不了
- 逃不掉
- 打不垮

- 访问控制机制等
- 授权机制等
- 加密机制等
- 数字签名、公证等
- 审计、监控等
- 数据备份和恢复等

# 网络安全体系结构

## ❖三维安全空间

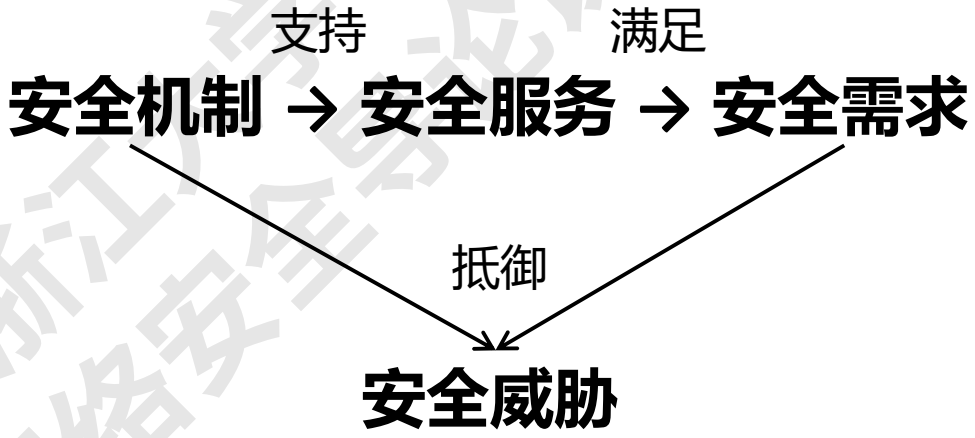
- 三个主要特性：
- 安全特性
- 结构特性
- 系统单元



# 网络安全体系结构

## ❖ISO/OSI安全结构

- **目标：**从管理和技术上保证安全策略得到准确地实现，**安全需求**得到全面准确地满足，确定必要的**安全服务**、**安全机制**和安全管理，以及它们在系统上的合理部署。



# 客观题

设置

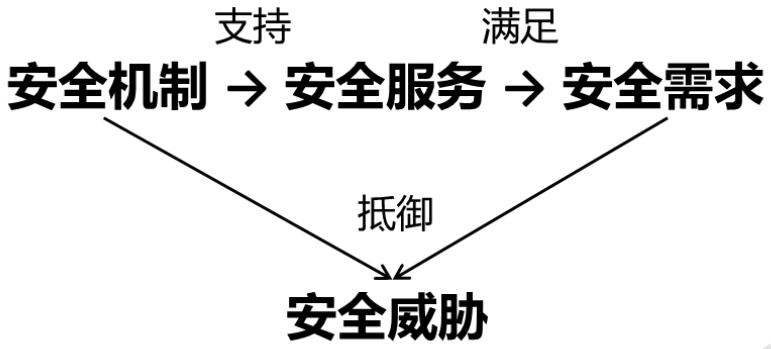
OSI（Open System Interconnect）参考模型包括哪七个层次?



作答

# 网络安全体系结构

## ❖ISO/OSI安全结构







**其他安全机制：**

- 可信计算
- 安全标记
- 事件检测
- 审计追踪
- 态势感知等

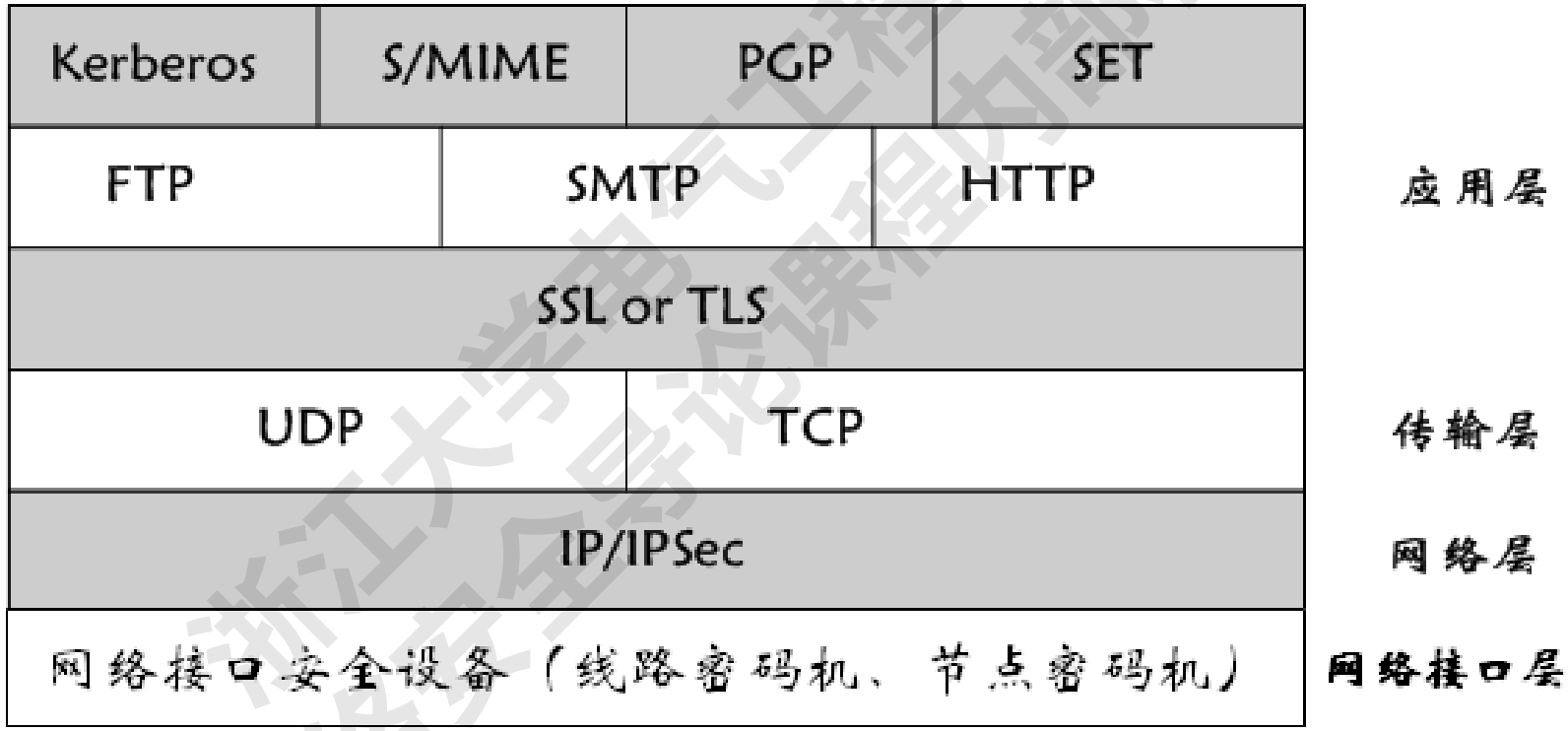
# 网络安全体系结构

## ❖ISO/OSI安全结构：安全服务与安全机制的关系

| 安全服务 | 安全机制 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 加密 | 数字签名 | 访问控制 | 数据完整性 | 身份鉴别 | 业务流填充 | 路由控制 | 公证 |
| 认证服务 | Y | Y | - | - | Y | - | - | - |
| 访问控制服务 | - | - | Y | - | - | - | - | - |
| 机密性服务 | Y | - | - | - | - | Y | Y | - |
| 完整性服务 | Y | Y | - | Y | - | - | - | - |
| 抗否认服务 | - | Y | - | Y | - | - | - | Y |

# 网络安全体系结构

## ❖TCP/IP安全体系框架

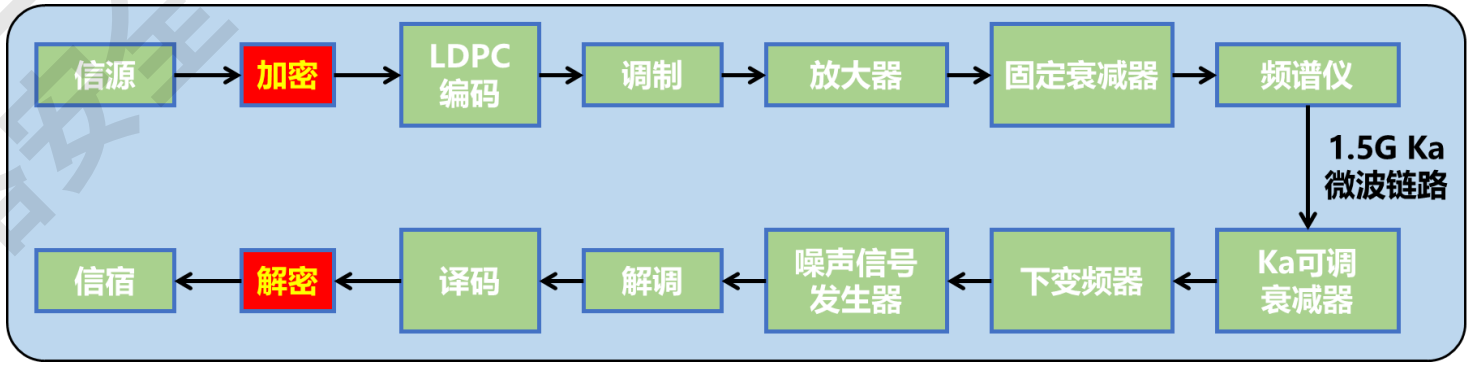


# 网络安全体系结构

## ❖TCP/IP各层实现安全服务的比较

### （1）网络接口层

- **优点**：独立于上层协议，为上层协议提供无缝安全服务，透明性好；能够通过硬件实现，效率高；
- **缺点**：与物理设备相关，难以实现，难以标准化；无法实现复杂的安全服务，一般仅实现专业的安全功能（例如，加密）。



## ❖TCP/IP各层实现安全服务的比较

### （2）网络层

- **优点**：透明性好，独立于上层协议，为上层协议无缝提供安全服务，同时也能够实现和物理设备的无关性；
- 网络层实现的安全服务，可被大量的上层协议共享，降低系统安全服务开销；上层协议为TCP/UDP；
- 伸缩性好，适用能力强，可解决端到端安全，也可解决点到点安全；
- **缺点**：较细粒度安全服务的支持；
- 实现难度大。

## ❖TCP/IP各层实现安全服务的比较

### （3）传输层

- **优点**：与应用协议透明性，独立于上层协议，能为上层协议无缝提供安全服务；
  上层协议：应用协议，如 HTTP；
- 针对性较强，可有效解决端到端的安全问题；
- **缺点**：保护范围有限。

- 传输层安全相应的协议：SSL(Secure Sockets Layer), TSL(Transport Layer Security), WTLS(Wireless Transport Layer Security)

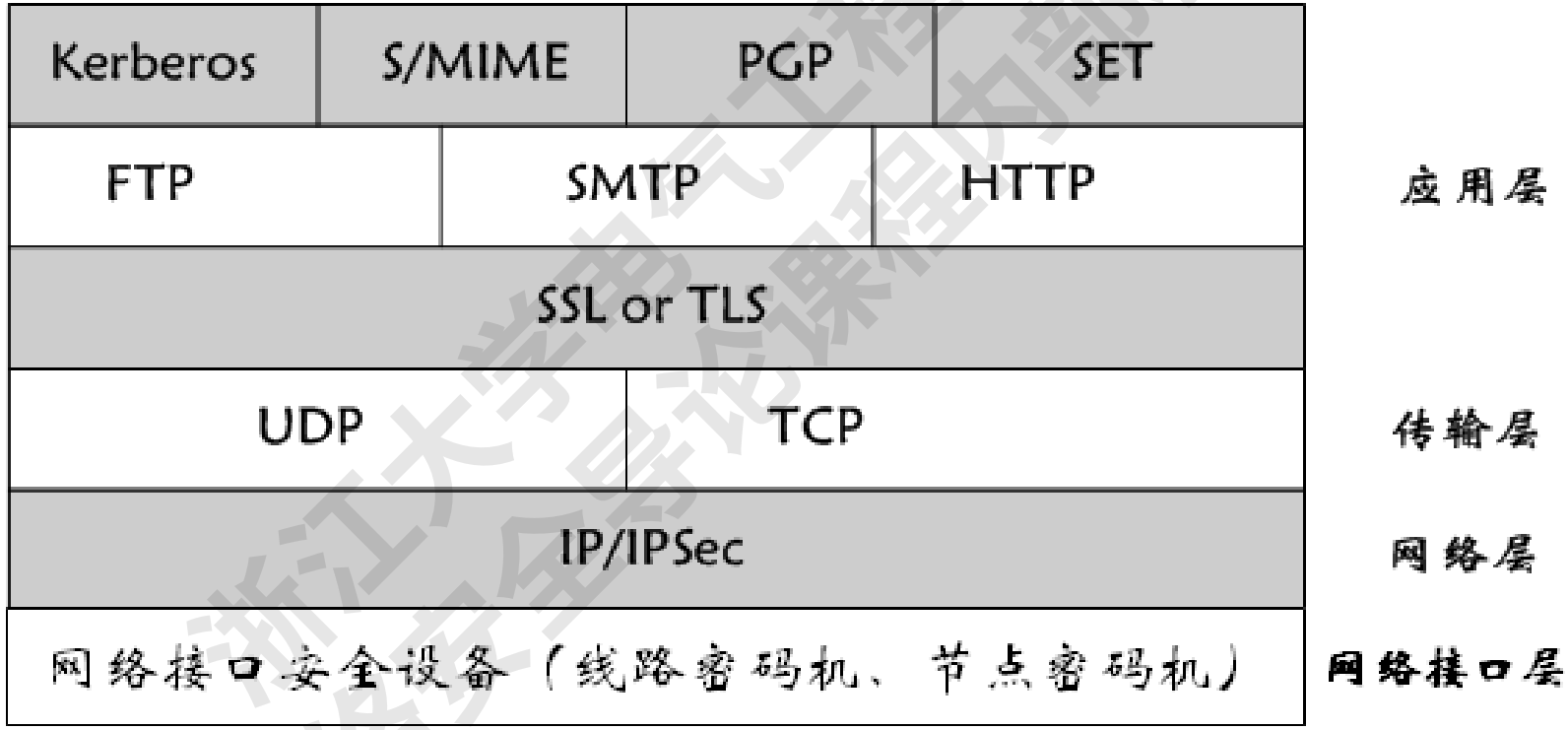
## ❖TCP/IP各层实现安全服务的比较

### （4）应用层

- **优点**：针对性强，可有效减少功能冗余；
- 容易访问与用户相关的用户个性数据；
- 可以提供特定的安全服务；
- 安全功能扩展性强。
- **缺点**：透明性差，安全体系的部署对现有应用影响很大；
- 每个应用都有各自的安全体系，安全体系很难保持一致。

# 网络安全体系结构

## ❖TCP/IP各层实现安全服务的比较




- **层级越高，实现起来相对容易，对应用的透明性越差；**
- **层级越低，实现起来相对困难，对应用的透明性越好。**

# 网络安全模型

❖**传统网络安全模型：** 对网络进行风险分析，制定相应的安全策略，采取安全技术作为防护措施。

- **以防为主**；
- **静态防护；**
- **被动防护**。

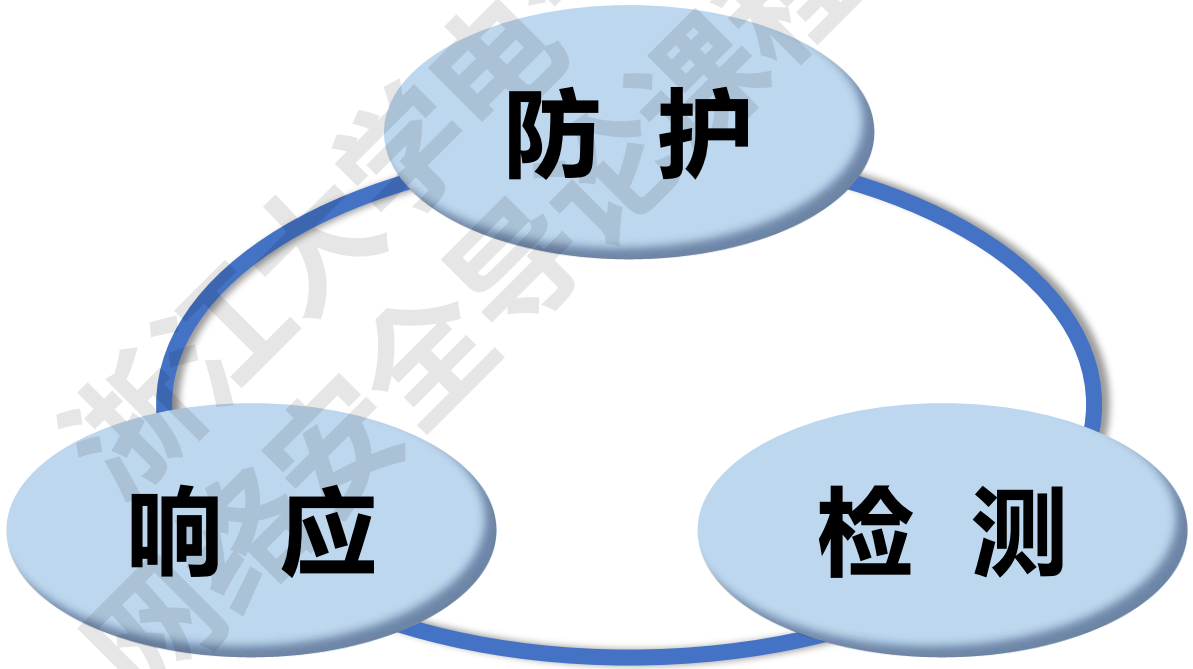
PDR模型

- **问题：**传统的安全模型要成功依赖于完善的防御手段和对系统正确的配置，并且很大程度上是针对固定的威胁和环境弱点。

# 网络安全模型

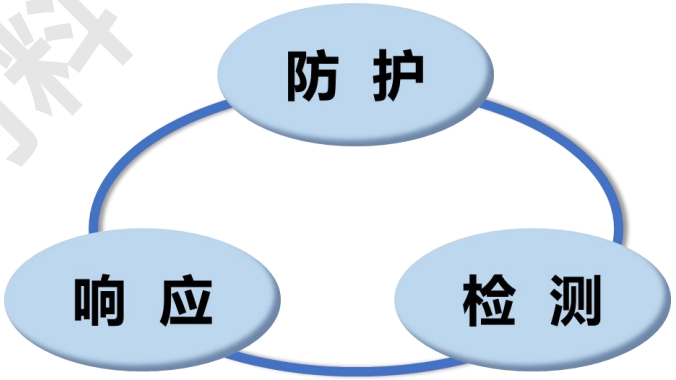
## ❖PDR模型

- 基于防护（Protection）、检测（Detection）、响应（Response）的安全模型。



# 网络安全模型

## ❖PDR模型




### （1）保护 (Protection)

- 针对目前已知的面临的安全威胁，采取一些保护措施；
- 措施：身份认证、访问控制、信息存储与传输安全、防火墙、VPN、防病毒等。
- **特点**：可抵抗大多数入侵事件的发生，但是不能够抵抗所有入侵事件，特别是利用新的系统漏洞（零日漏洞，zero-day vulnerability），新的攻击手段的入侵。

## ❖PDR模型

### （2）检测 (Detection)

- 措施：漏洞扫描、实时监控、入侵检测、安全审计等。
- **事前**：漏洞扫描，发现系统安全漏洞和隐患；
- **事中**：入侵检测，实时发现入侵行为（已知和未知）；

  IDS (intrusion detection system)
- **事后**：安全审计，记录系统中的事件，以查证是否发生入侵事件和用于事后追踪。

# 网络安全模型

## ❖PDR模型

### （3）响应 (Response)

- 目标：对安全事件作出快速反应，尽量减少和控制对系统影响的程度。
- 措施：漏洞修补、报警、中止服务、数据备份与容灾等。
- **特点**：
- **一是动态防护；**
- **二是主动防护。**

- **传统：**
- **以防为主；**
- **静态防护；**
- **被动防护。**

# 网络安全模型

## ❖PDR模型

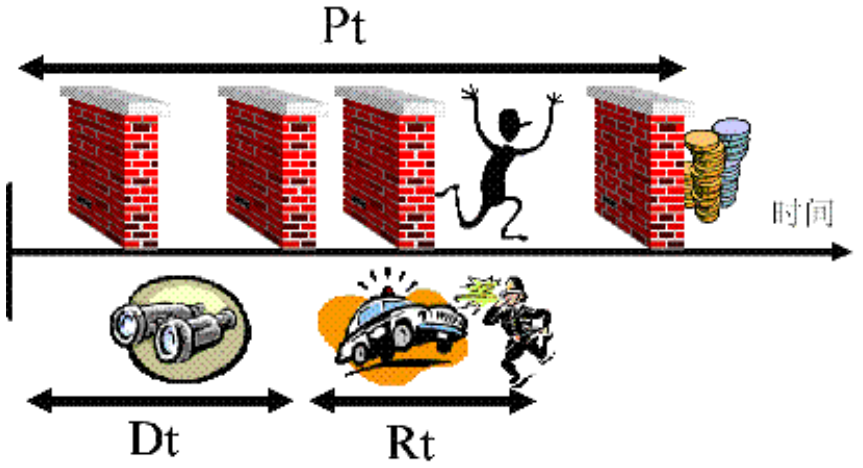
- **基本原理：**相关活动（攻击、防护、检测、响应）都要消耗时间。简单来说，可用时间来衡量一个体系的安全性和安全能力。

- **Pt > Dt + Rt**

**Pt**：系统为保护安全目标设置各种保护的防护时间；或理解为**在该保护方式下入侵者攻击目标所花时间**；

**Dt**：从开始入侵到系统能检测入侵行为所花时间；

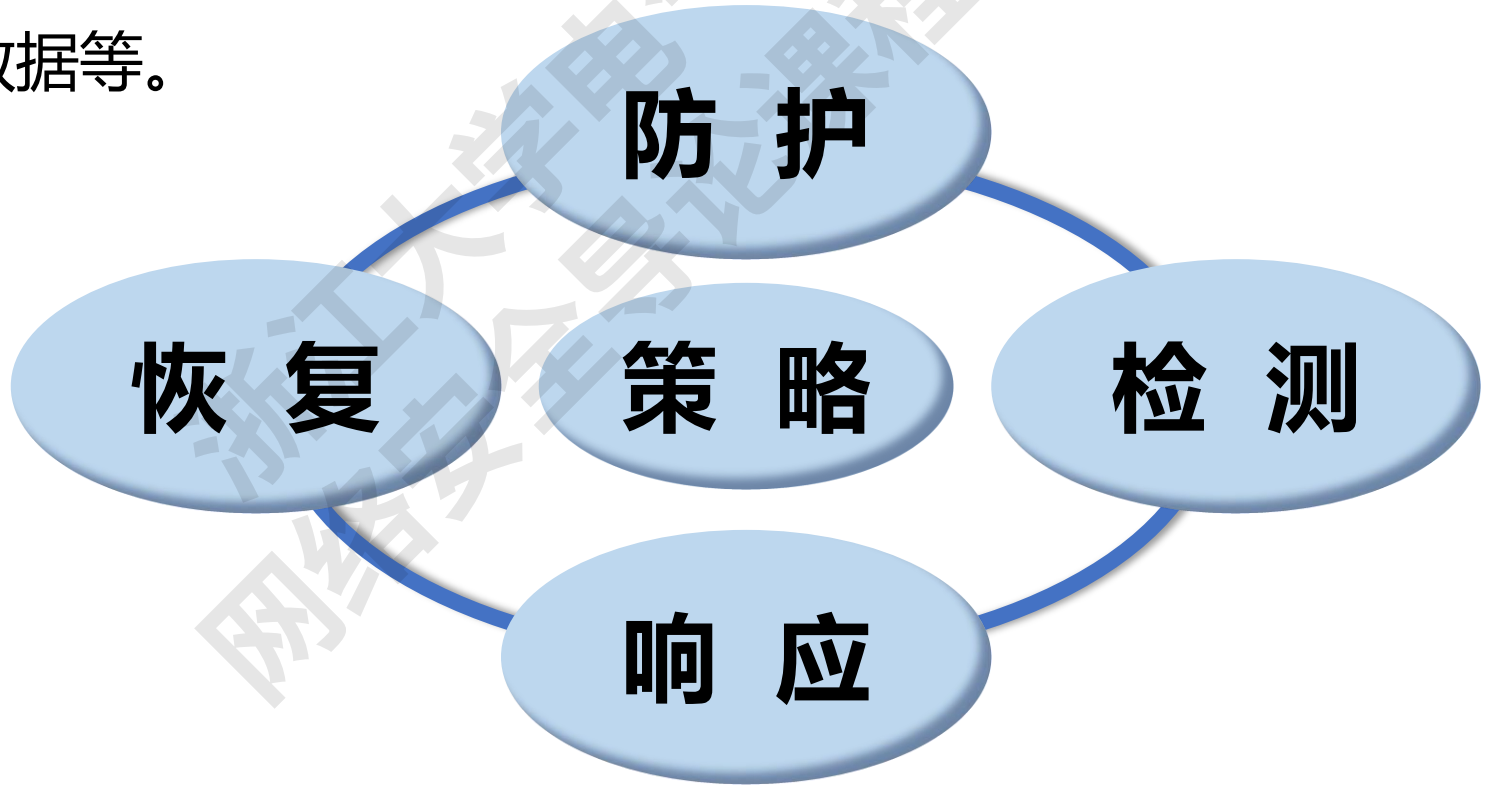
**Rt**：发现入侵开始系统能够做出足够的响应所花时间。



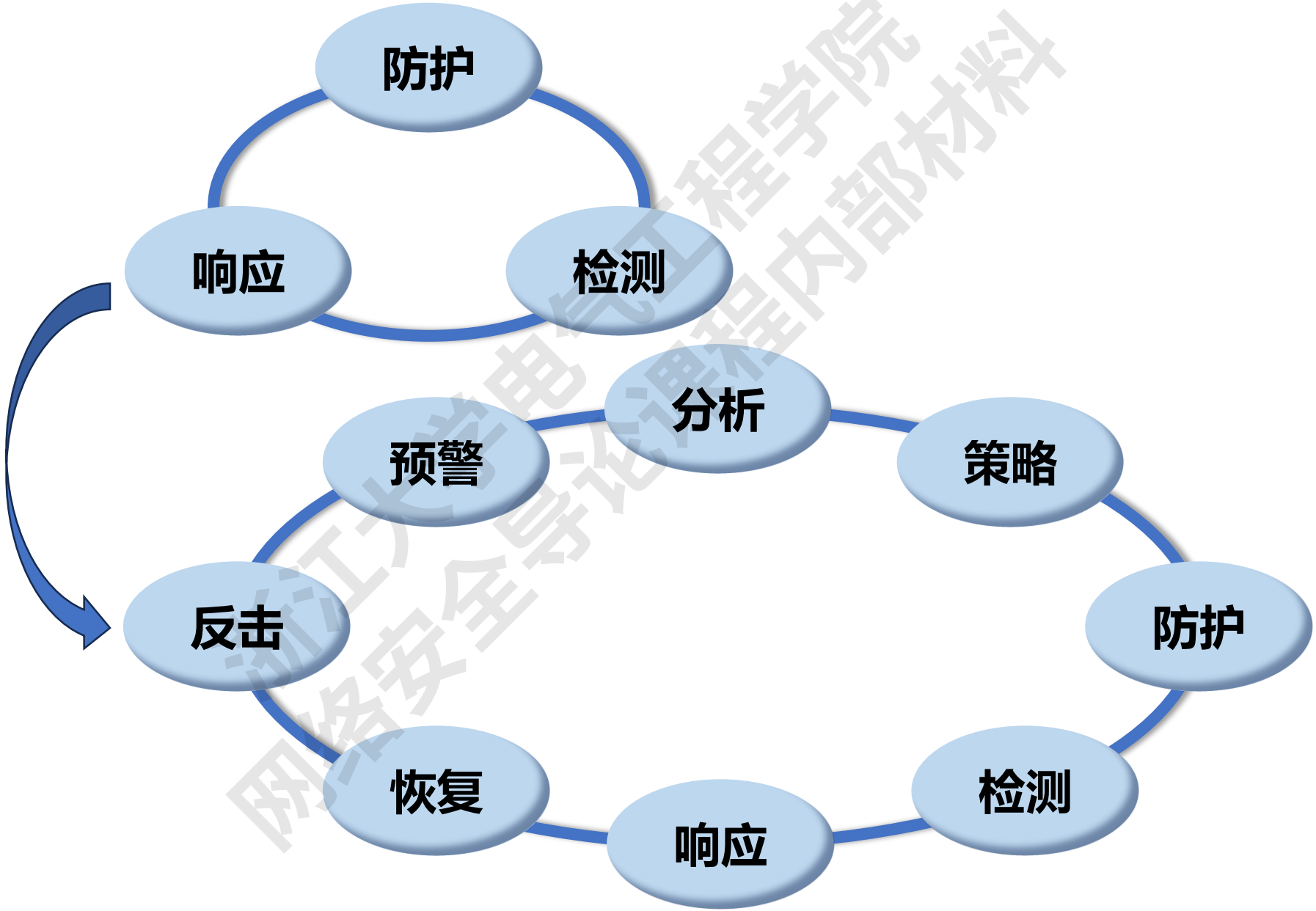
# 网络安全模型

## ❖PPDRR模型

- PPDRR模型是在 PDR 模型的基础上新增加了 **Policy （策略）** 、**Recovery （恢复）**，这样一旦系统安全事件发生了，也可以恢复系统的正常运行，恢复系统功能和数据等。



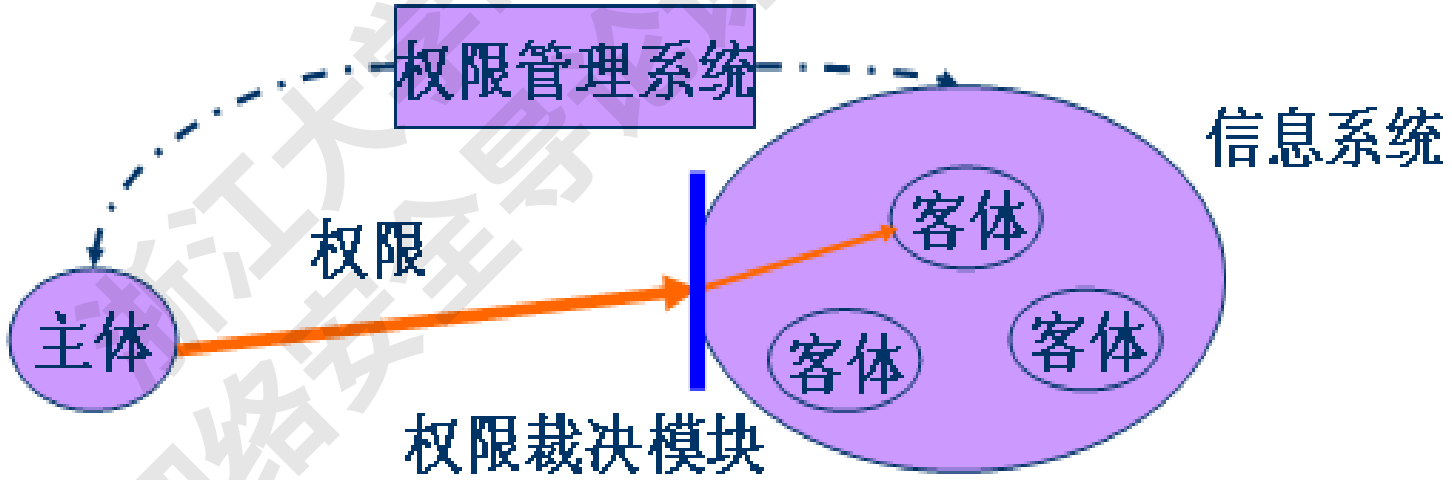
# 网络安全模型



# 网络安全防御策略/原则

## ❖最小特权策略

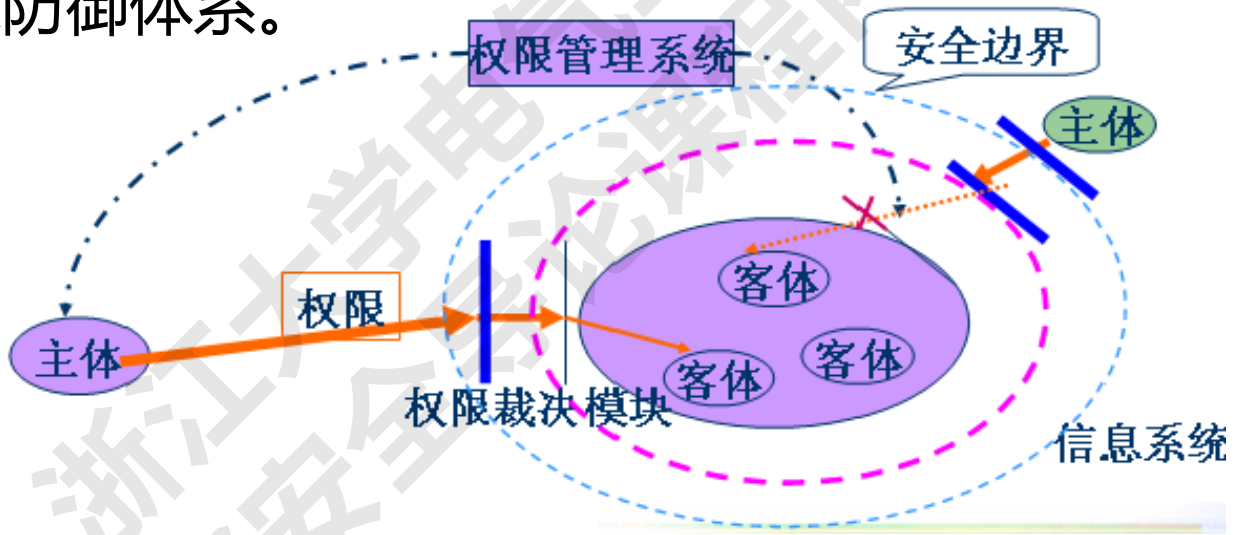
- 主体仅具有其完成特定任务所必需的权限，此外没有任何其它权限。所谓权限，指的是主体对客体的操作能力的集合。



# 网络安全防御策略/原则

## ❖纵深防御策略

- 安全体系是由多个安全边界构成，各安全边界既相互独立地完全任务，又相互配合构成纵深防御体系。

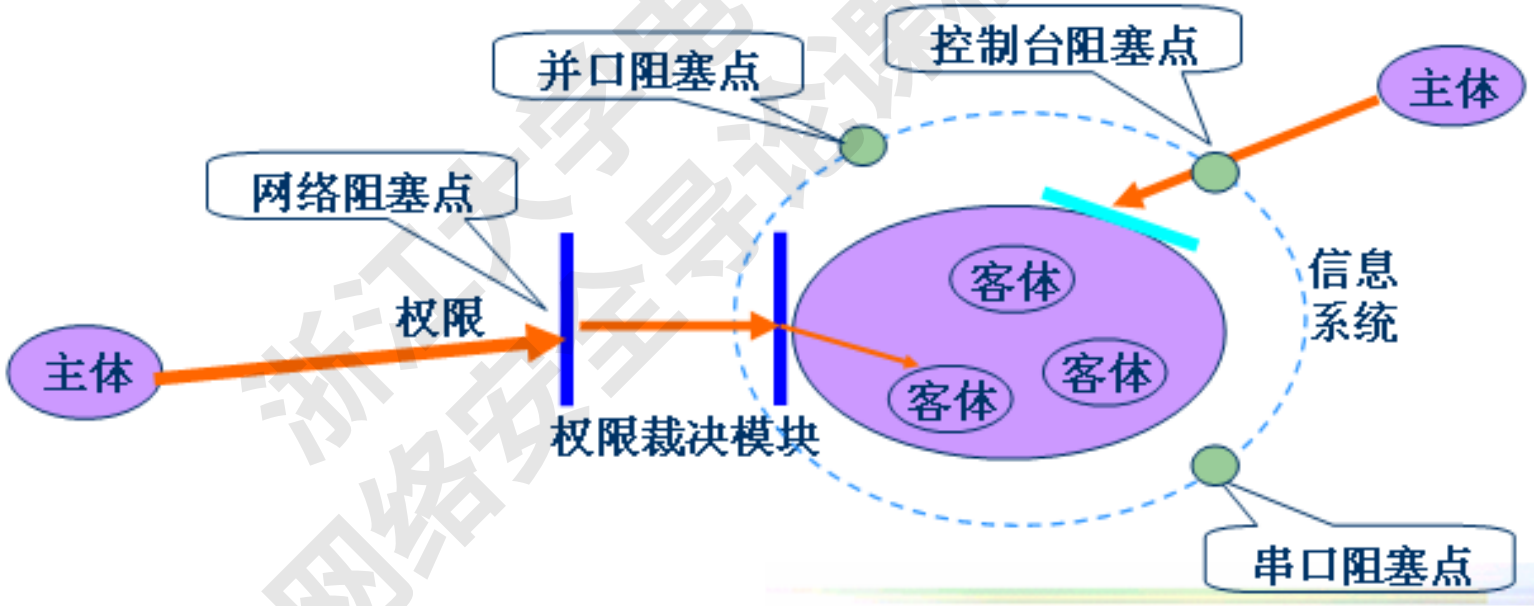



- 主体要访问信息系统中的客体，需要经过网络边界、主机边界，直至访问到内部数据；
- 单一的网络边界防护因控制粒度仅限于网络地址级，所以有可能造成非授权访问现象出现；
- 所以需要在各安全边界间构成一个不同粒度的纵深防御体系，才能对重要信息进行有效的安全防御。

# 网络安全防御策略/原则

## ❖阻塞点防御策略

- 阻塞点是信息系统中可以被系统管理员进行监控和连接控制的点。 在阻塞点进行控制，防止第三方的攻击。

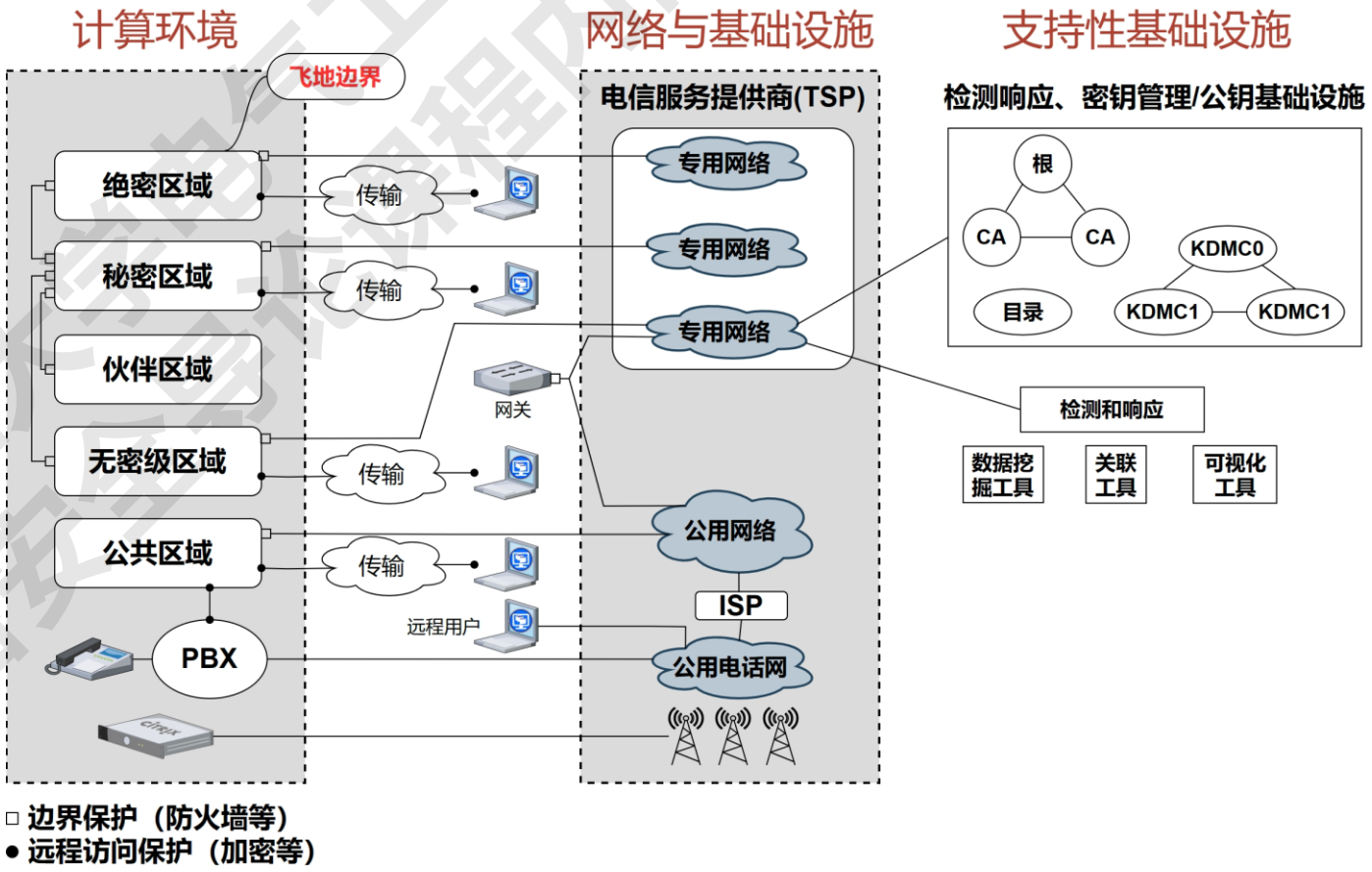


# 网络安全保障技术框架

## ❖信息保障技术框架（IATF）

- 美国国家安全局（NSA）发布，从技术层面分为四部分：

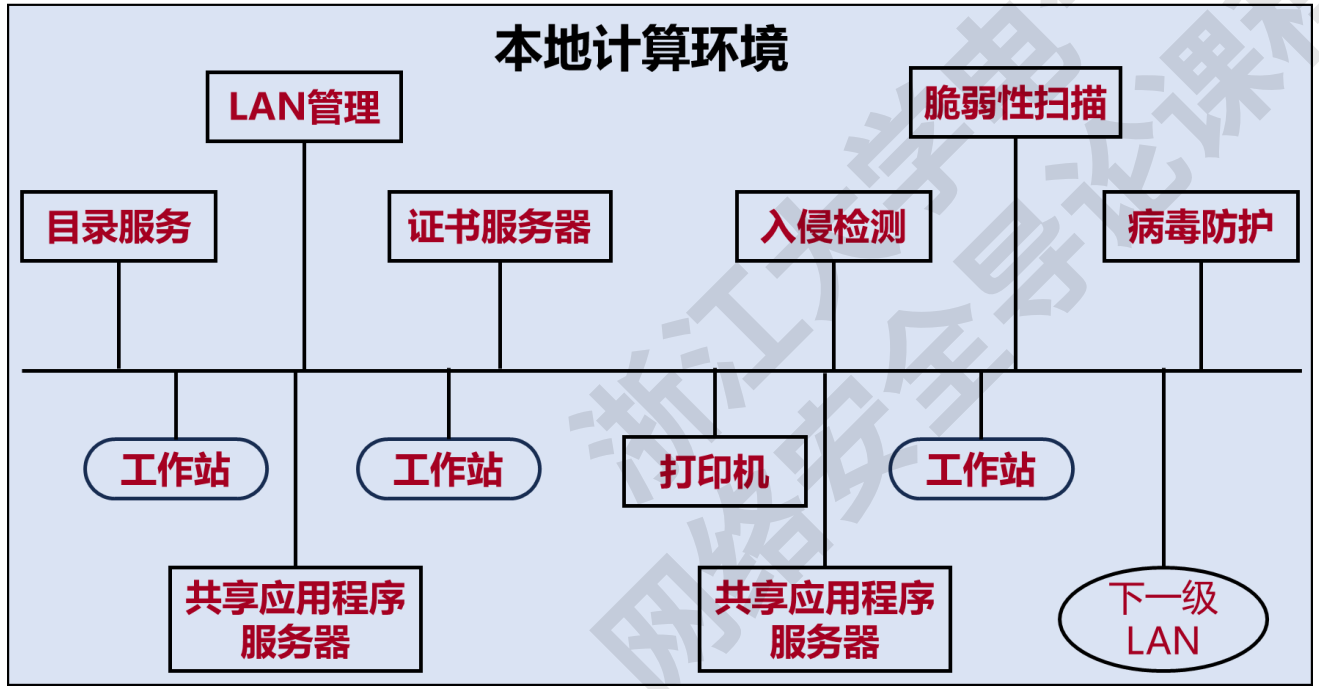
- **本地计算环境**
- **本地计算环境边缘（飞地边界）**
- **网络与基础设施**
- **支持性基础设施**



# 网络安全保障技术框架

## ❖信息保障技术框架（IATF）

- **本地计算环境：包括服务器、客户机及其上所安装的应用程序。**




**计算环境安全：**

- 操作系统安全
- 数据库安全
- 病毒升级服务
- 终端安全服务等

# 网络安全保障技术框架

## ❖信息保障技术框架（IATF）

- **飞地边界**

- “飞地” 指的是在局域网内部、采用单一安全策略，并且不考虑物理位置的**本地计算设备的集合**。

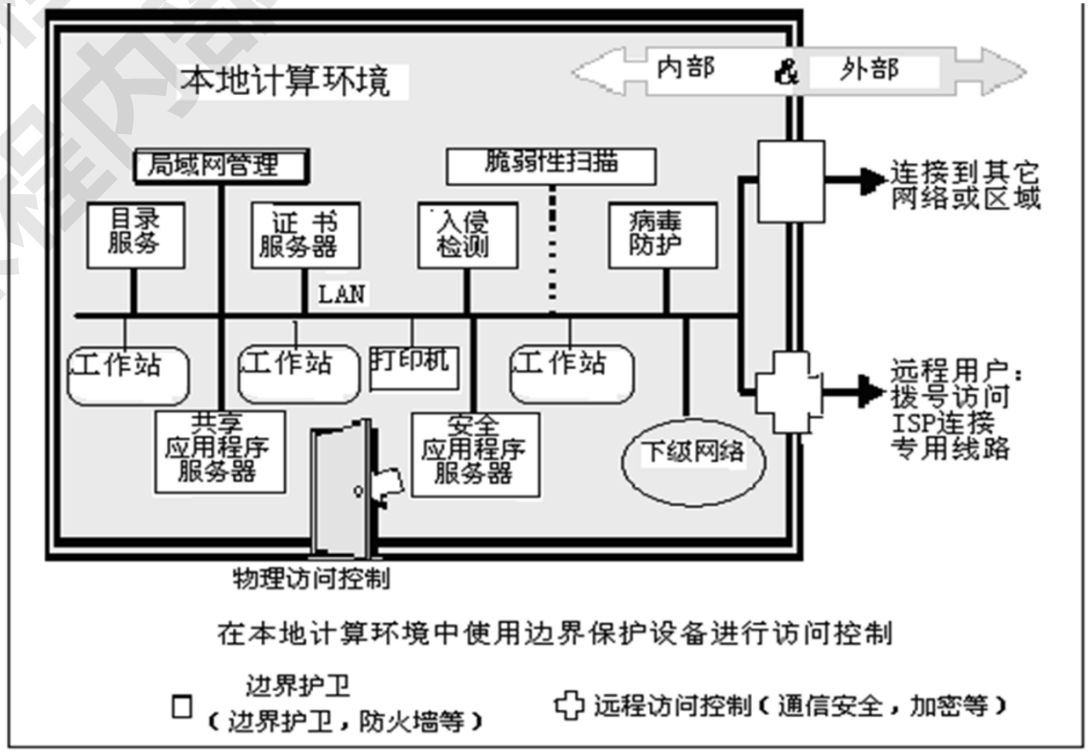
- 本地和远程元素在访问某个飞地内的资源时必须满足该飞地的安全策略要求。

# 网络安全保障技术框架

## ❖信息保障技术框架（IATF）

- **飞地边界**
- 飞地边界是信息进入或离开飞地的位置。
- 飞地边界处常采用多种方式的外部网络连接。

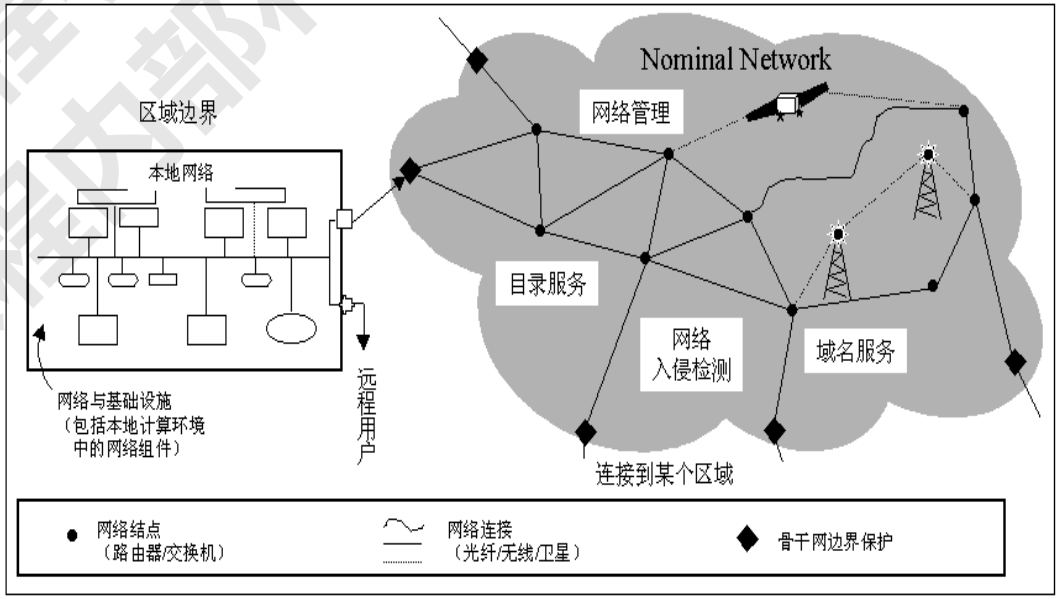
**飞地边界安全**：除去本地计算环境的安全防护外，还应包括**远程安全互联**、**安全边界防护**等。



# 网络安全保障技术框架

## ❖信息保障技术框架（IATF）

- **网络与基础设施:** 提供飞地互连。
- 信息传输组件（例如卫星、微波、其他广播频率频谱与光纤）。
- 网络管理、域名服务器和目录服务等。



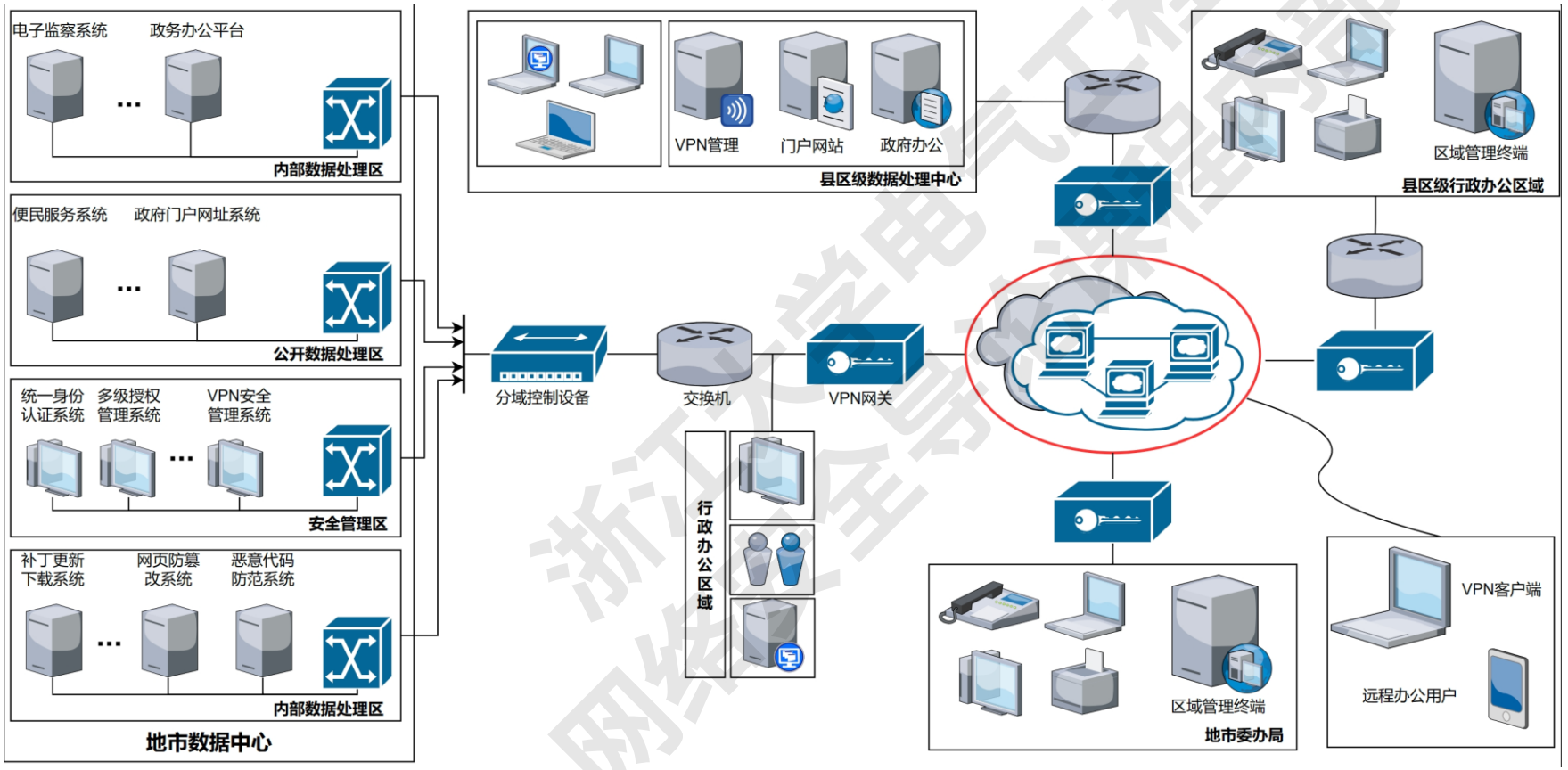
# 网络安全保障技术框架

## ❖信息保障技术框架（IATF）

- **支撑性安全基础设施**
- 为本地计算环境、飞地边界、网络与基础设施中的计算机、服务器、应用等信息系统提供这类安全服务的一套相互关联的基础设施。
- 负责提供密钥与证书管理服务；能够对入侵和其它违规事件快速进行检测与响应，并能够支持操作环境的入侵检测、报告、分析、评估和响应等。
- IATF 包括的安全基础设施：**密钥管理基础设施** (KMI/ PKI)；**检测与响应基础设施**。

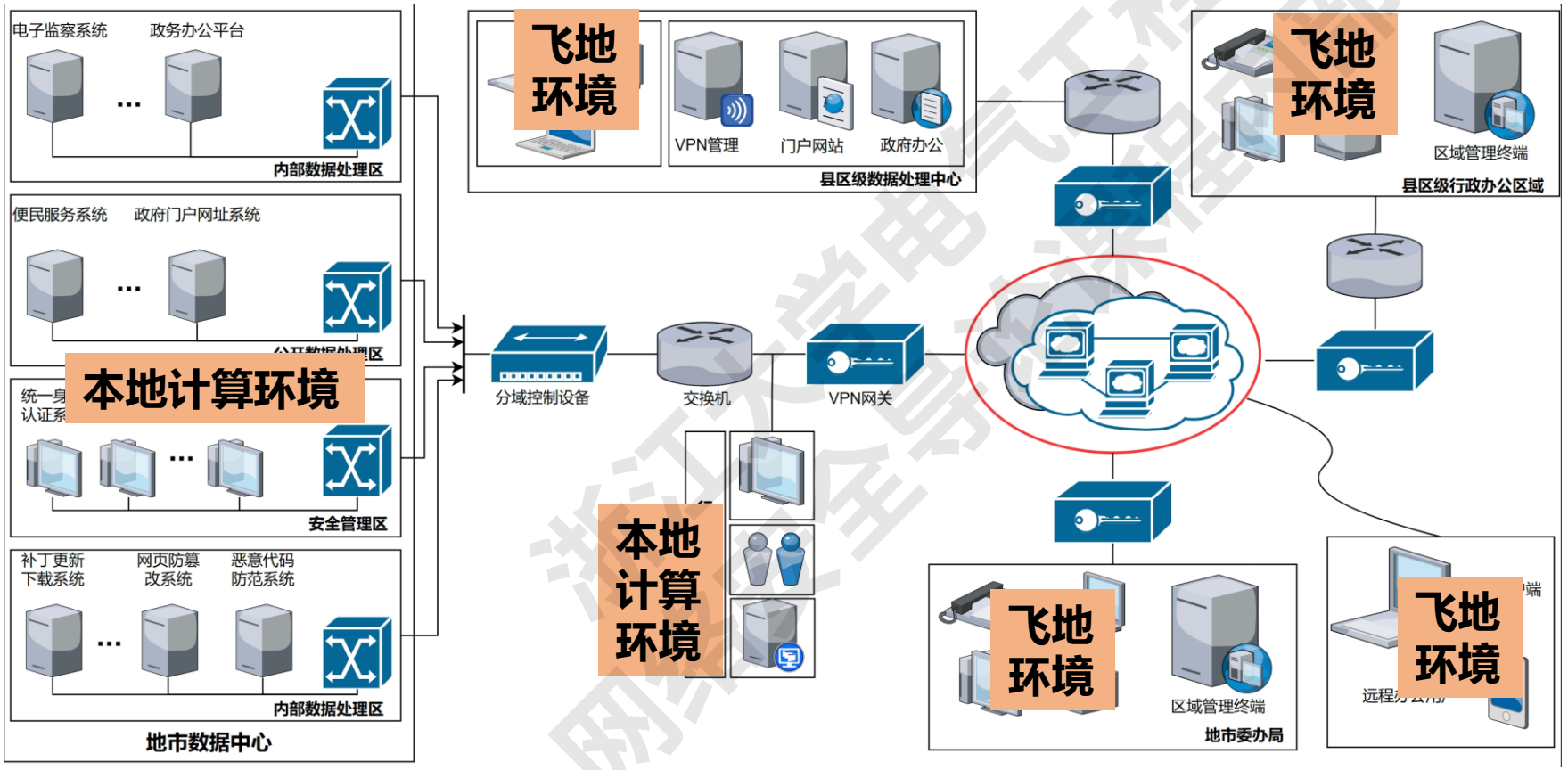
# 网络安全保障实例

## ❖互联网电子政务信息安全保障



# 网络安全保障实例

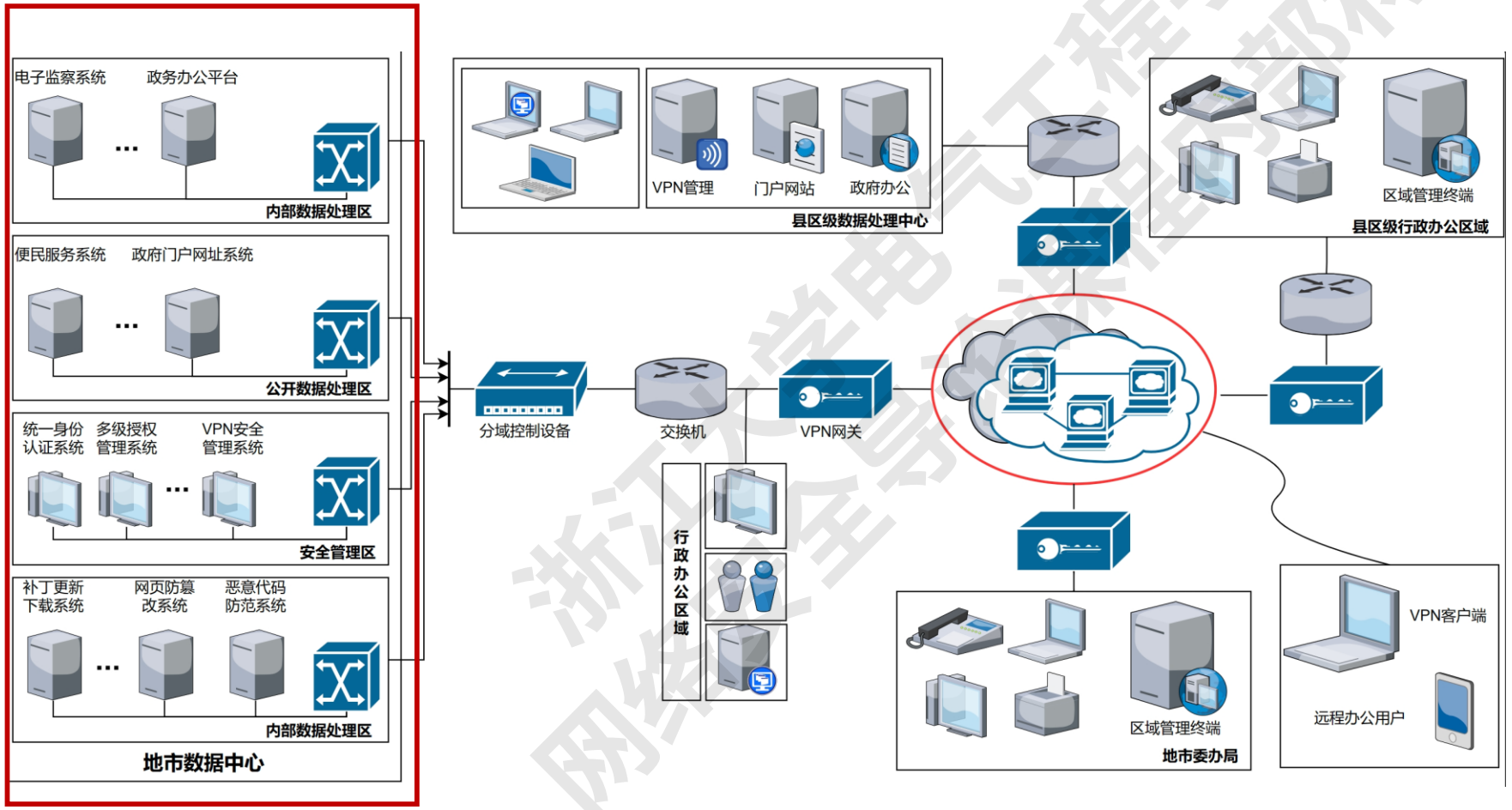
## ❖互联网电子政务信息安全保障




- 互联区域中地市数据中心、地市委办局处于地市本地区域可以称之为本地计算环境。
- 其它地方是系统中的飞地环境。

# 网络安全保障实例

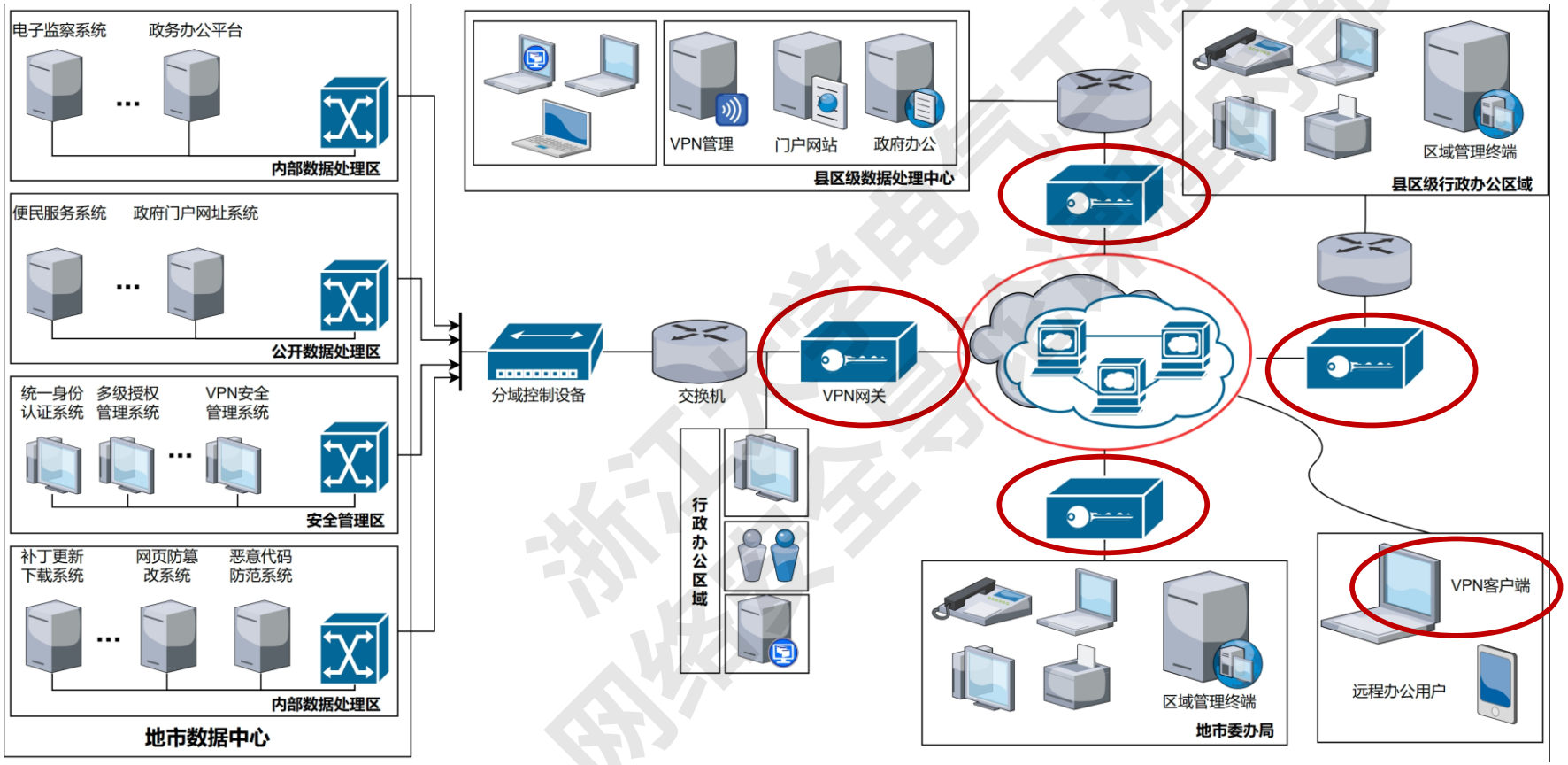
## ❖互联网电子政务信息安全保障




- 安全管理区中的多级授权管理系统等，等价于IATF中的PKI和KMI所提供的功能与服务。
- 补丁更新等系统，等价于检测与响应基础设施的部分功能。

# 网络安全保障实例

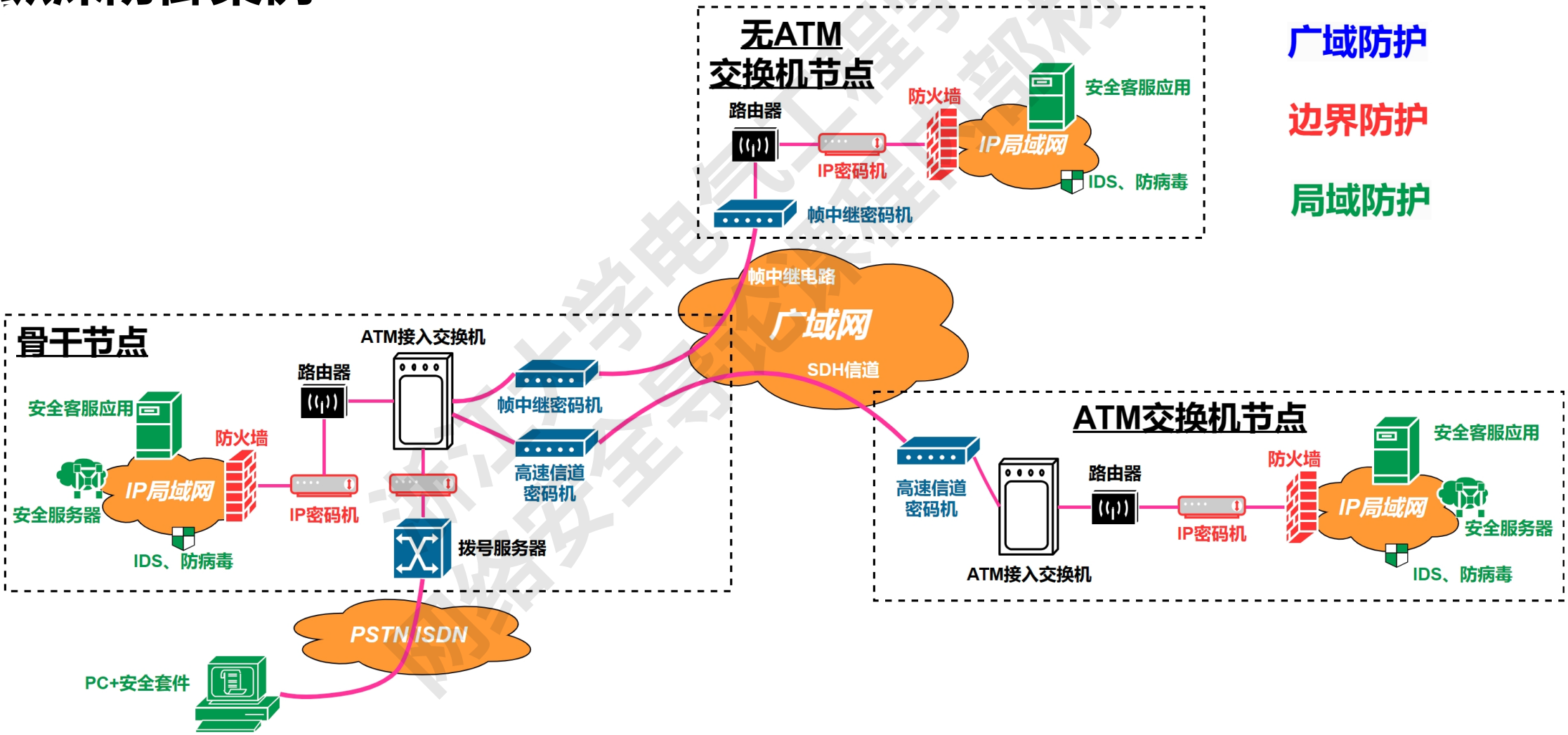
## ❖互联网电子政务信息安全保障




- VPN安全网关、VPN客户端通过综合采用密码技术、安全隧道技术、安全管理技术等，实现各区域间的网络安全互联，保证区域间信息传输的保密性与完整性。

# 网络安全保障实例

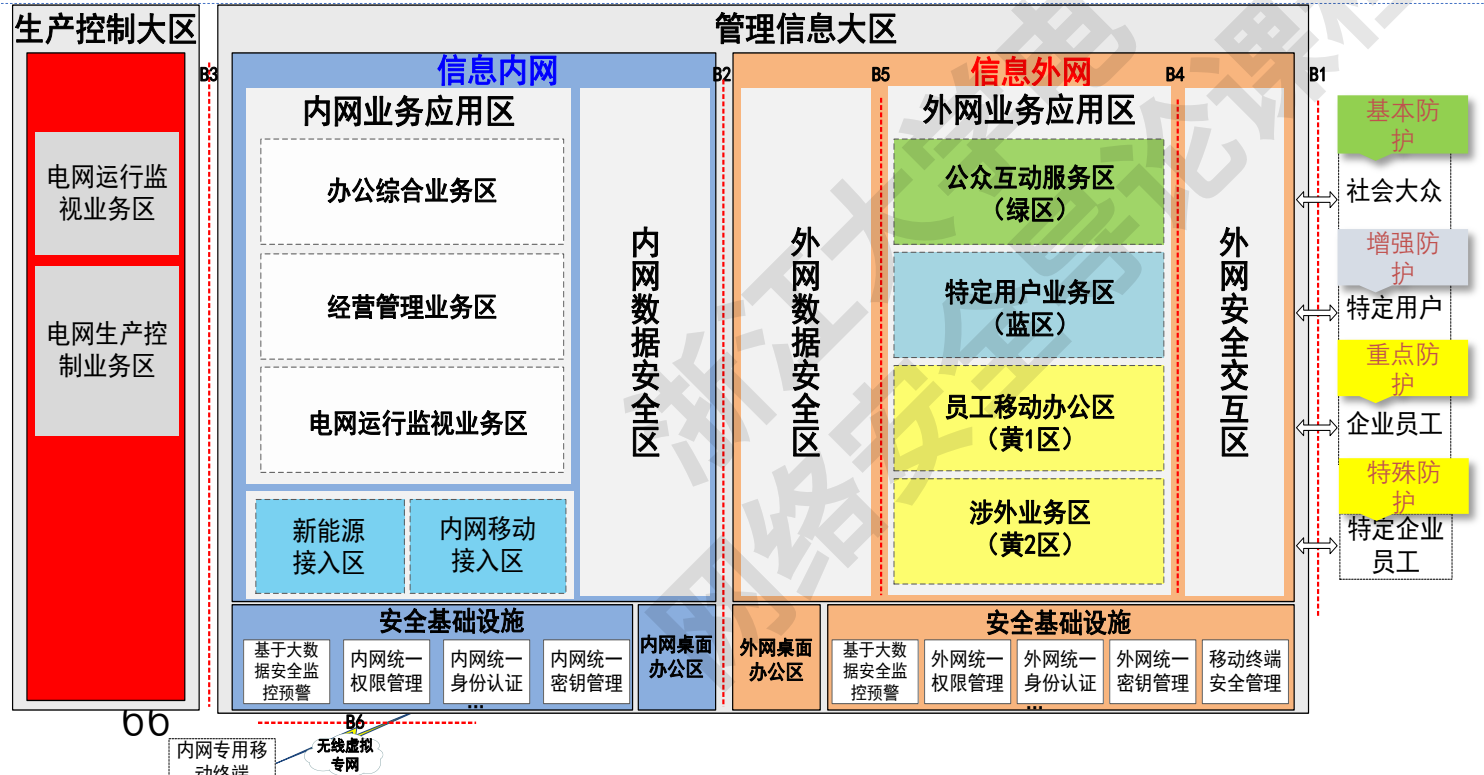
## ❖纵深防御案例



# 网络安全保障实例

## ❖电力系统网络安全防护

- 电力网络安全一直受高度关注，2002年行业内提出了“安全分区、网络专用、横向隔离、纵向认证”的电力二次安全防护体系，重点强化了网络边界隔离保护，“十三五”期间，国网公司制定了“可管可控、精准防护、可视可信、智能防御”的安全策略，在“十二五”主动防御体系基础上，强化网络安全的全周期管控、多层次可信、全方位感知、人员技术保障，构建完成网络安全智能防护体系。





2002年5月30号令


2004年12月5号令

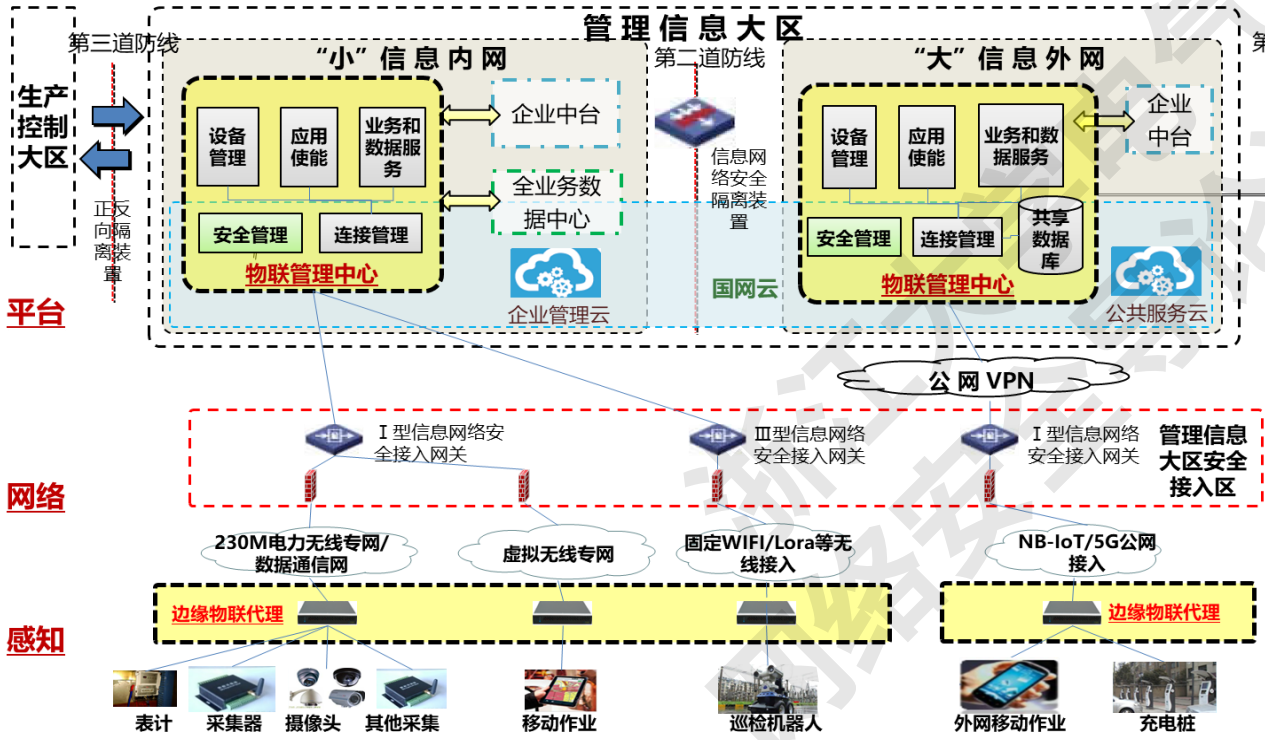

2014年8月14号令


2015年2月

# 网络安全保障实例

## ❖电力系统网络安全风险

- 随着能源互联网的建设推进，“大云物移智链”等新技术得到广泛应用，电网业务模式发生变革，海量异构终端广泛接入，网络边界模糊、数据交互多元，使得电力系统在各环节均面临着**感知层、网络层、平台应用层安全**风险。




**平台应用层**

**数据交互共享**

电网数据价值日益凸显，在数据交互共享需求下保障数据安全成为难点

**网络层**

**万物智慧互联**

面对万物智慧互联，网络边界模糊，终端身份管理机制和密钥基础设施尚未匹配

**感知层**

**海量设备接入**

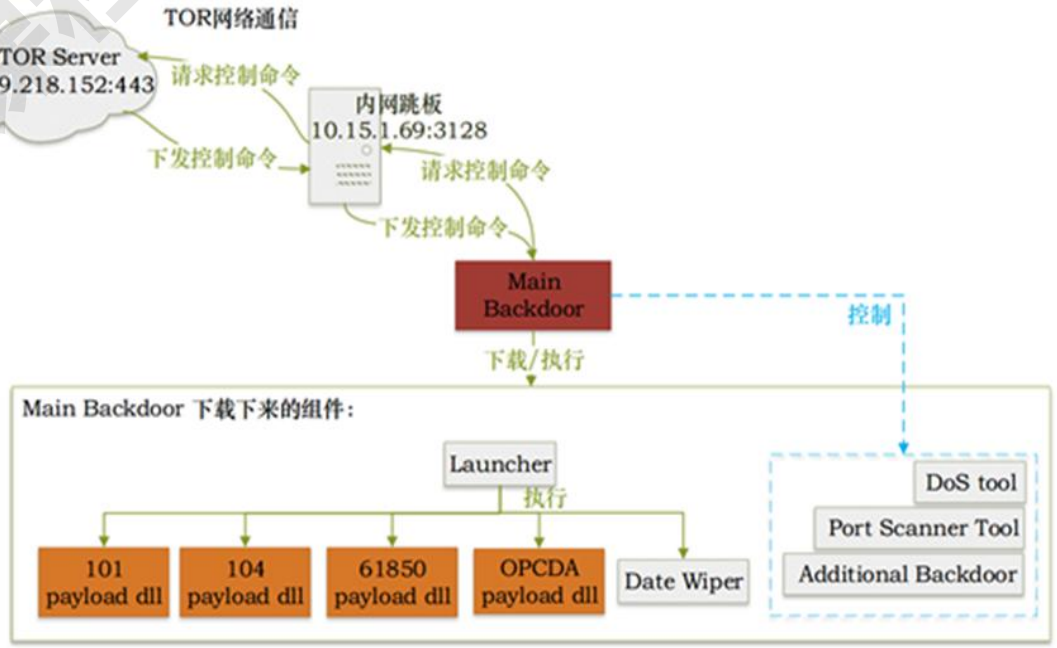
电网设备数量指数级扩张，面对海量异构终端接入，安全与性能难以平衡

网络与信息安全风险来自**企业内、外部**，覆盖电力系统**全业务环节**

# 网络安全保障实例

## ❖电力系统网络安全风险 -- 网络层案例

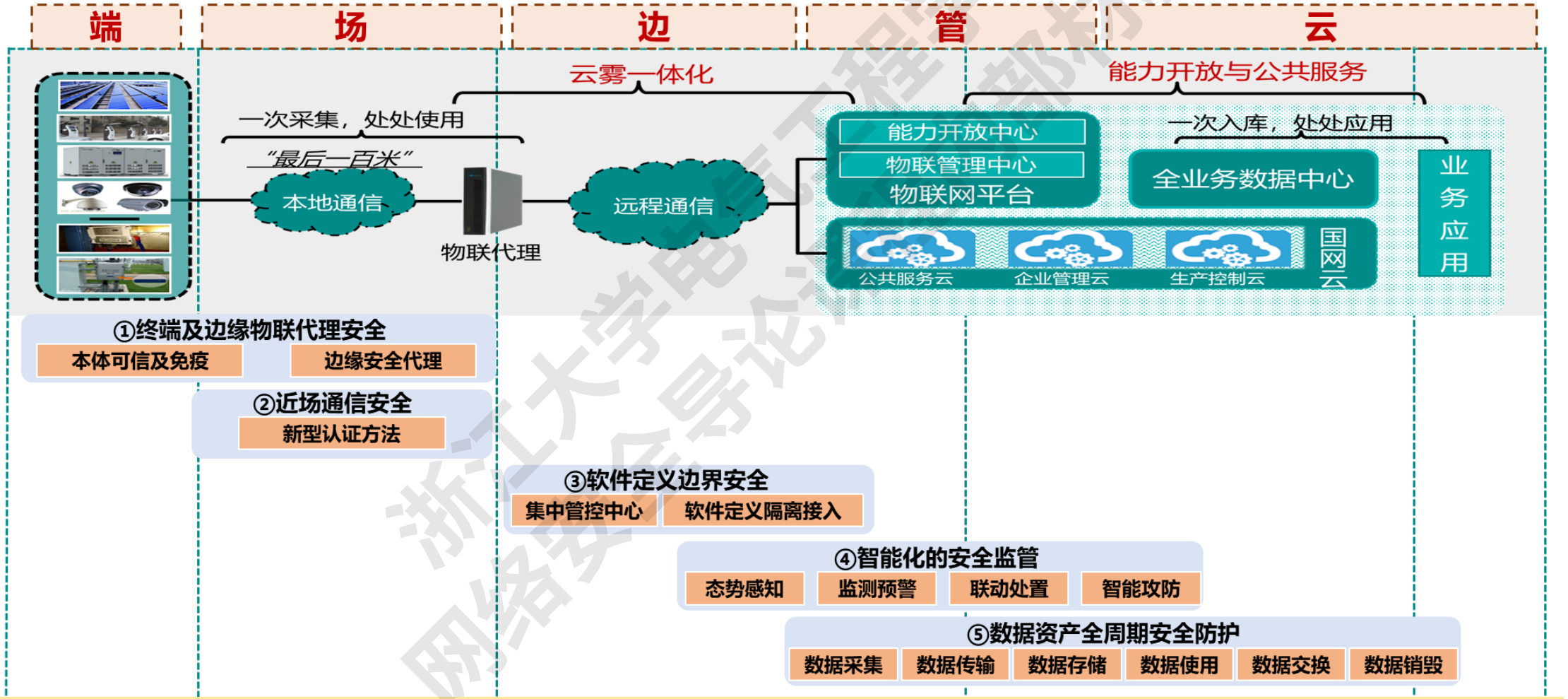
- 工业网络通信协议的安全设计相对不足。2017年6月，国外发现针对电网设备的“Industroyer”恶意软件，该恶意软件利用通用工业通信协议在安全认证机制上的缺失，随意篡改控制指令，可以无限循环打开关闭断路器，从而对全球近百个变电站智能终端进行控制。




**电力工控协议在设计之初安全性考虑不足**

# 网络安全保障实例

## ❖电力系统网络安全风险 -- 纵深防御




**电力网络联动智能防御体系**

# 网络安全基础研究框架


检验
系统攻击与安全评测
信息系统的安全应用
手段
监控管理
基础
安全体系结构
桥梁
安全协议与认证
核心
密码理论与技术
保证
安全芯片

# 课程小结

- 网络安全威胁事件
- 网络安全的发展与演变
- 网络安全内涵 （“是什么”）
- 网络安全体系结构 （“是什么”）
- 网络安全模型 （“做什么”）
- 网络安全防御策略/原则 （“怎么做”）
- 网络安全保障技术框架、实例

# 一个通讯游戏

假定两人赌博决定胜负，最常用的办法是抛硬币.

通常规则是：一人选定一面，另一人抛硬币．不妨假定乙选定一面，甲抛硬币．如果乙选定的一面出现，则乙胜出，否则甲胜出.

请注意：上述游戏必须两人面对面进行.

规 定：两人以上进行的游戏规则，通常我们称为协议．一人可以执行的规则，只能称为程序.



来源：www.icourse163.org，厦门大学慕课《信息安全》

# 一个通讯游戏

协议的特点： 协议中的每个人都必须了解协议，并且预先知道所要完成的所有的步骤。

协议中的每个人都必须同意并遵循它。

协议必须是清楚的，每一步必须明确定义，并且不会引起误解。这就要求协议的表诉一定要精确无误。



来源：www.icourse163.org，厦门大学慕课《信息安全》

# 一个通讯游戏

我们的问题是：如果两人不是面对面，通过电话或者其它通讯手段，如何执行上述协议？

因为上述协议能够进行的前提是：两人面对面进行．如果甲在电话上说:你选一面，我来抛并告诉你是否赢了．乙会同意吗？

为了在通讯中(电话中）完成这个游戏， 需要修改上述协议．密码学家想出一个办法，在协议中增加密码技术．这个密码技术依赖下述奇妙的数学函数：



来源：www.icourse163.org，厦门大学慕课《信息安全》

# 一个通讯游戏

我们的问题是：如果两人不是面对面，通过电话或者其它通讯手段，如何执行上述协议？

因为上述协议能够进行的前提是：两人面对面进行．如果甲在电话上说:你选一面，我来抛并告诉你是否赢了．乙会同意吗？

为了在通讯中(电话中）完成这个游戏， 需要修改上述协议．密码学家想出一个办法，在协议中增加密码技术．这个密码技术依赖下述奇妙的数学函数：



来源：www.icourse163.org，厦门大学慕课《信息安全》

# 一个通讯游戏

**定义 1.1**

一个函数 $f(x)$称为单向函数，如果满足以下两条性质：

1. 对任意整数 $x$，由 $x$ 计算 $f(x)$ 是容易的. 而给出 $f(x)$，要找出对应的原像 $x$是不可能的，不管 $x$ 是奇数还是偶数.
2. 不可能找出一对整数：

$$x \neq y, f(x) = f(y)$$

注意：这里的词“容易”和“不可能”需要严格的数学表述，即给出某种量化的表达方式. 以后我们会说明这一点，因为它们反映了安全性. 这种函数的存在性问题也需要进一步讨论.



来源：www.icourse163.org，厦门大学慕课《信息安全》

# 一个通讯游戏

现在假定这样一个单向的函数 $f(x)$ 已经找到，双方同意以偶数代表正面，奇数代表反面．我们可以制定一个电话抛币的协议：

**协议** 1.2

电话掷币．假定：双方同意

1. 具有定义*1.1* 的单向函数 $f(x)$；
2. 偶数 $x$ 代表正面，奇数 $x$代表反面；

然后执行

1. 甲选择一个大随机数 $x$,计算 $f(x)$，然后通过电话告诉乙 $f(x)$的值；
2. 乙告诉甲，对 $x$ 的奇偶性的猜测；
3. 甲告诉乙 $x$ 的值；
4. 乙验证 $f(x)$，从而看出他所作出的猜测是正确或错误的．



来源：www.icourse163.org，厦门大学慕课《信息安全》

# 主观题 1分

设置

请同学们分析下上述协议的合理性，即协议的安全性。



作答

# 一个通讯游戏

上述游戏能够进行，关键有两点：

- 对甲而言：无法（从计算上看非常困难）找到两个奇偶性不同的数：

$$x \neq y, f(x) = f(y)$$

因此乙愿意执行这个协议；

- 对乙而言：依据 $f(x)$ 的值，他没有可以利用的资源猜测或非常难于计算 $x$ 的值，或他猜测奇数或偶数的概 率都是 $\frac{1}{2}$，所以甲愿意执行这个协议。

因此我们说，依据上述协议，游戏对双方是公平的.



来源：www.icourse163.org，厦门大学慕课《信息安全》

# 一个通讯游戏

- 计算的困难性保证了双方在游戏中的安全；数学上的**计算困难性**是安全得到保障的基础；
- 一个数学问题不能在合理时间解决，就称为困难问题；
- 增加密码技术的协议，为安全密码协议；协议1.2的存在性依赖**单向函数**的存在性；
- 保证通信安全**不能仅靠数学特性**，例如，电话掷币时，还要有电话录音、身份鉴别、第三方公证等。有的依赖数学方法，有的依赖物理设备。

来源：www.icourse163.org，厦门大学慕课《信息安全》