



西安电子科技大学  
XIDIAN UNIVERSITY

# 无线网络安全融合的架构与关键技术

马建峰

西安电子科技大学

2017.09



## 研究背景



## 网络侧安全关键技术



## 数据侧安全关键技术



## 应用侧安全关键技术



## 一体化集成安全体系



## 主要工作进展



□ 5G、SDN、空天一体化等未来网络呈现出设备及系统智能化、异构融合、面向应用等基本特征。



2020 and  
Beyond Ad Hoc

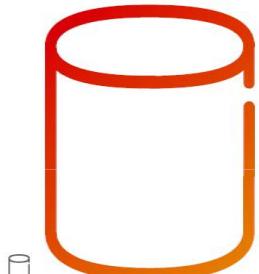
更高的数据容量  
Higher data capacity

海量设备连接  
Mass-device connection

更高的峰值速率  
Higher peak rates

更低的时延  
Lower latency

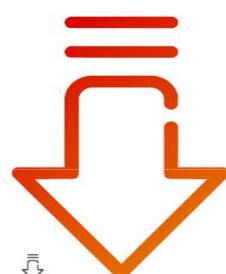
更低的能耗和成本  
Lower energy consumption and costs



1000x



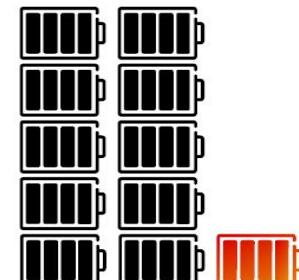
10-100x



10-100x



5x

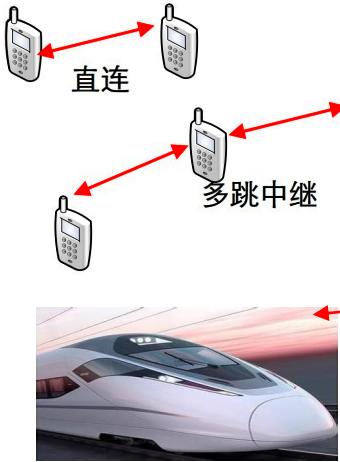


10x



## 新终端

New Terminal



## 新技术

New Technology

网络层  
融合

数据层  
融合

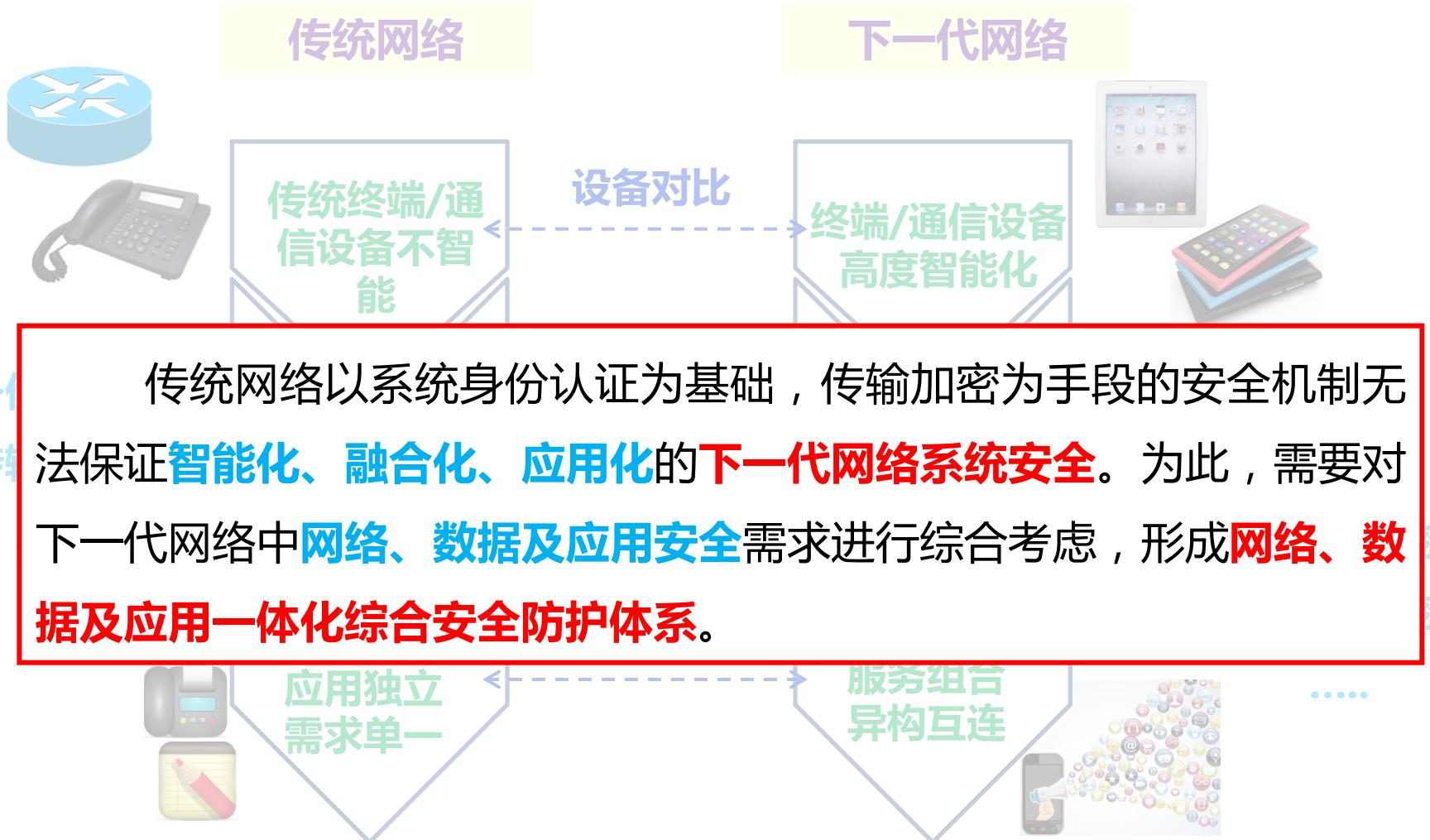
应用层  
融合



终端智能化

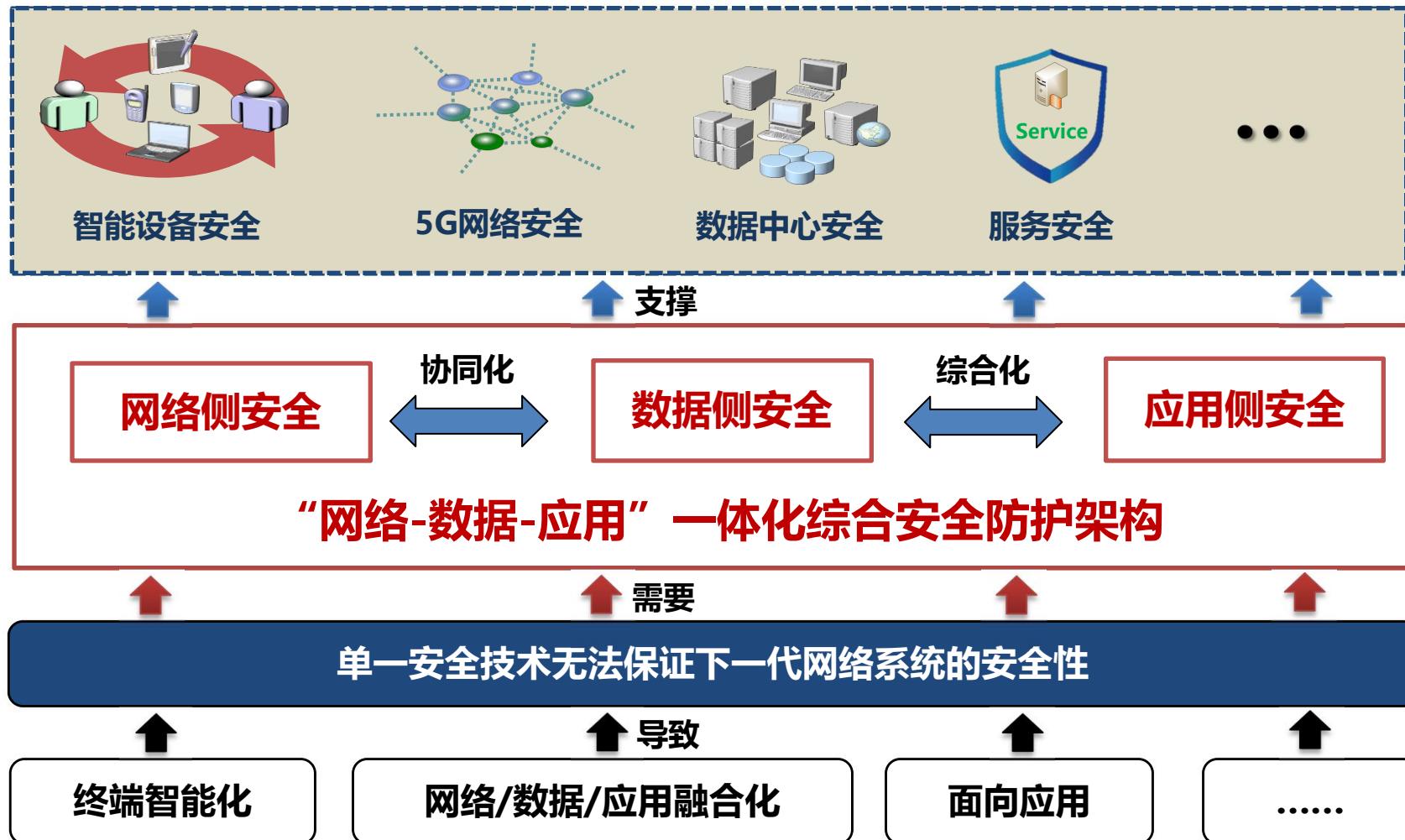
网络/数据/服务融合

面向应用





□ 新终端、新技术、新业务使得下一代网络安全挑战更加严峻。下一代网络系统更加复杂，因此需要综合考虑**网络、数据、应用**多种安全机制。





## ◆ 研究背景

## ◆ 网络侧安全关键技术

## ◆ 数据侧安全关键技术

## ◆ 应用侧安全关键技术

## ◆ 一体化集成安全体系

## ◆ 主要工作进展



终端系统智能化

多网络、多安全域

新型网络技术  
( NFV, SDN )

单一的身份认证及加密传输技术无法保证网络侧安全

智能设备系统安全

- 可信运行环境
- 分区分级管理
- 拟态安全防护
- 软件相似性检测....

异构网络安全融合

- 自适应多模接入认证
- 高效安全漫游切换
- 多因子认证....

新型网络  
安全防护技术

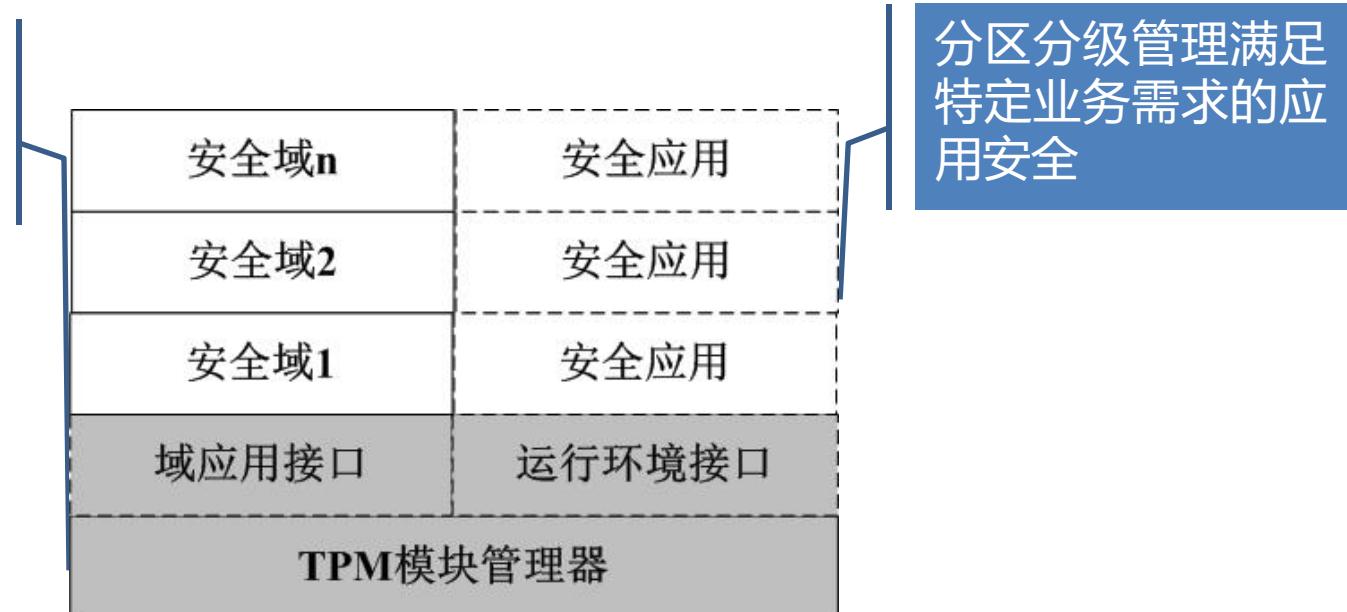
- NFV安全防护体系
- SDN安全防护体系
- ...



## □ 智能设备系统安全——可信运行环境

- 系统可信运行环境：采用**TPM技术**，实现**全生命周期的密钥管理、数字证书管理以及安全域的动态管理**，保证**实体认证、数据的机密性、完整性、不可否认性**。
- 分区分级管理：构建**基于可信模块的分区安全控制架构**及**多级安全控制方法**，实现**多任务系统强安全隔离和细粒度访问控制的需求**，提高**系统可靠性和安全性**。

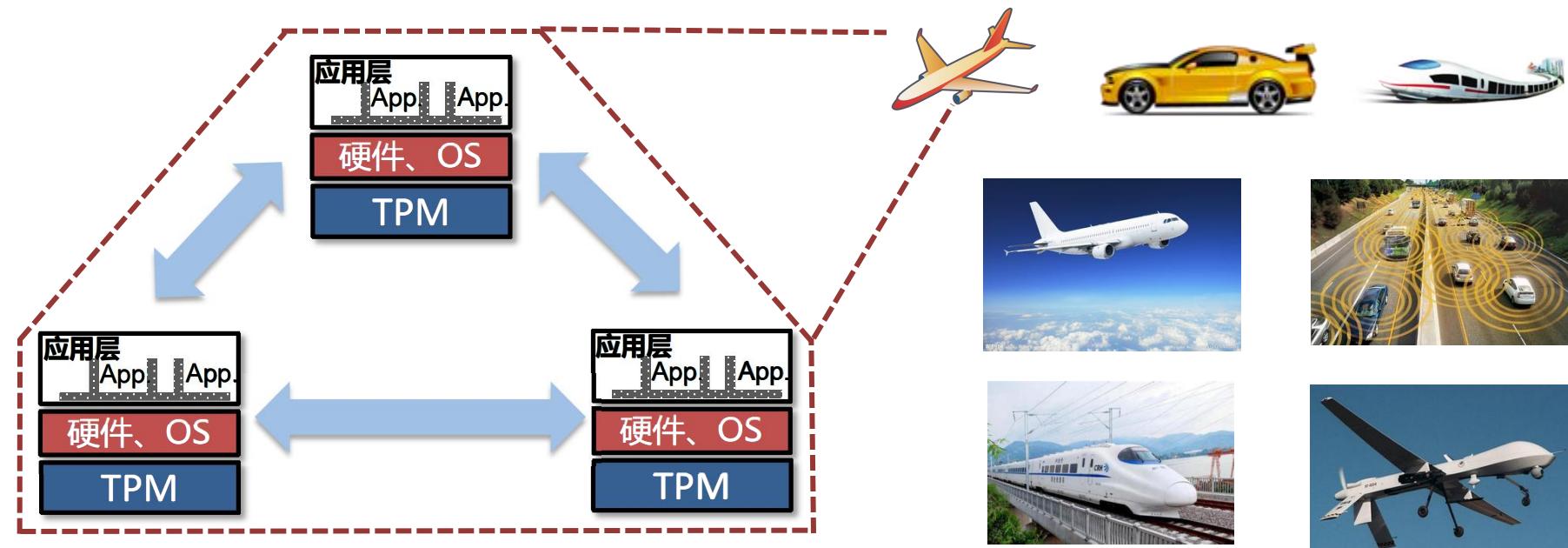
基于TPM模块提供设备认证、密钥管理、加解密等服务





## □ 智能设备系统安全—可信运行环境

- 集中式信任体系导致大规模系统中的**可信链过长（信任衰减大）**、系统完整性校验开销大等挑战。
- 研究方向：**基于分布式信任体系的可信运行环境**





## □ 智能设备系统安全

### ➤ 拟态安全

- 以异构冗余多模裁决机制**识别和屏蔽未知缺陷与未明威胁**；以系统的视角在不确定属性防御或拒止针对目标系统的不确定性威胁。
- 面临挑战：对于大规模系统，**多样冗余设计、策略变化管理困难**等

### ➤ 软件相似性检测

- 旨在检测软件的相似度，进而判断软件行为是否合法，还可以应用于**数字版权保护、恶意软件检测、软件漏洞挖掘**等软件安全性分析。
- 面临挑战：难以应对**代码混淆、多态**等规避技术；难以应用于**复杂的、大规模软件系统**中



## □ 网络安全和身份认证

- 身份认证是对用户、设备等的**真实性**进行验证，可广泛应用于系统、网络、应用等不同方面。

	方法	目的
系统层	口令、生物特征、设备特征等	进入系统、获取资源
网络层	密码学、基于口令证书等	接入网络
应用层	口令、生物特征、用户行为特征等	取得应用使用权限

- 在现今**智能化、融合化、应用化**的趋势下，仅采用单一身份认证机制无法保证各类网络系统/平台的安全性，不同层次身份认证技术**协同化、综合化**是未来的发展方向。



## □ 综合化身份认证技术（例：智能终端）

- **系统层认证**：开机（文本密码、手势密码、指纹识别）、root权限申请等
- **网络层认证**：连接WiFi（字符串口令密码、输入无线路由器PIN码）等
- **应用层认证**：访问应用（口令密码、短信验证、语音验证、二维码扫描）等

### 系统层认证



### 网络层认证



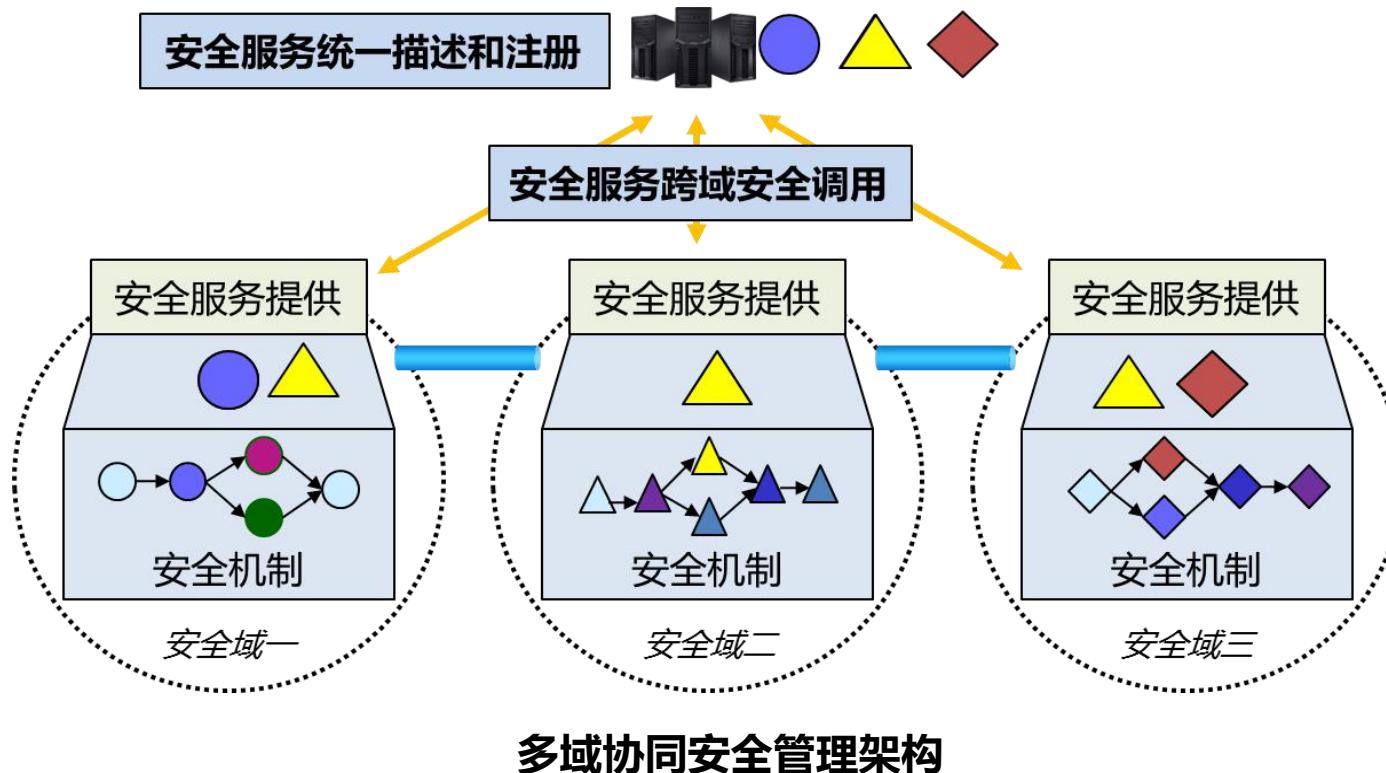
### 应用层认证





## □ 异构网络融合安全—异构多域协同安全管理架构

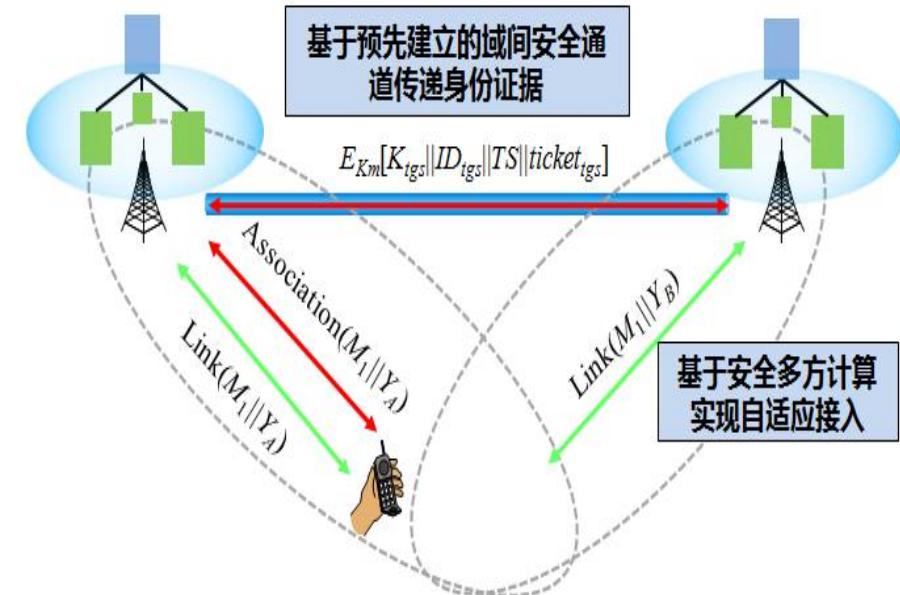
- 针对多种异构无线网络并存的特征，设计了**异构多域协同安全管理体系结构**，提出了**自适应安全接入、端到端安全传输**等关键技术。





## □ 异构网络融合安全—自适应安全接入方法

- 提出了基于已有安全证据和安全多方计算的**自适应接入认证方法**，实现了终端**自适应安全接入**。



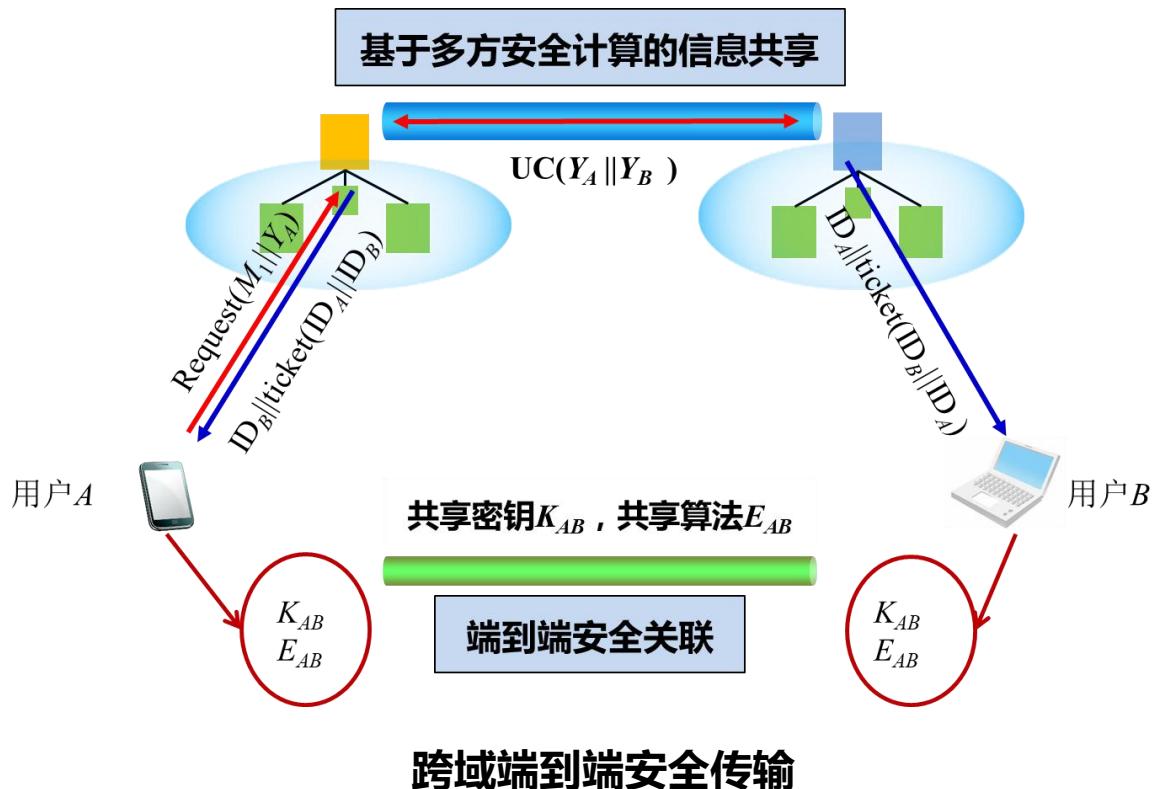
异构多域无线网络安全接入体系架构

自适应接入认证方法



## □ 异构网络融合安全——跨域端到端安全传输

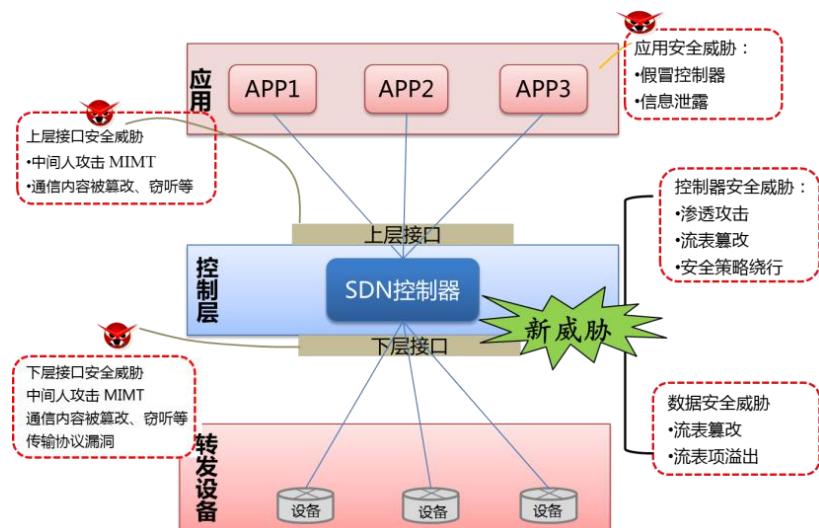
- 提出了**异构多域无线网络端到端认证/加密方法**，保证了**端到端信息交互的安全**。



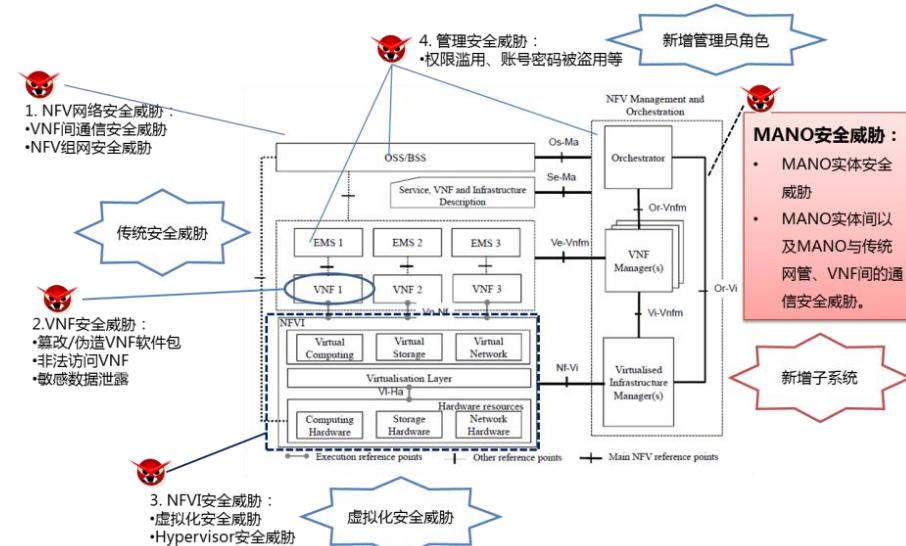


## □ 新型网络安全防护技术—SDN和NFV安全防护技术

- SDN使得网络硬件可编程化，并且可以集中式管理和控制；NFV旨在利用标准的IT虚拟化技术解决网络资源动态化问题。但目前仍缺乏成熟的技术应用，尚无具体的应用协议。
- 研究方向：一方面，在技术应用研发同时，**构建系统的安全体系**；另一方面，根据应用需求，针对**安全子集中的具体安全机制**开展深入研究。



SDN安全需求分析

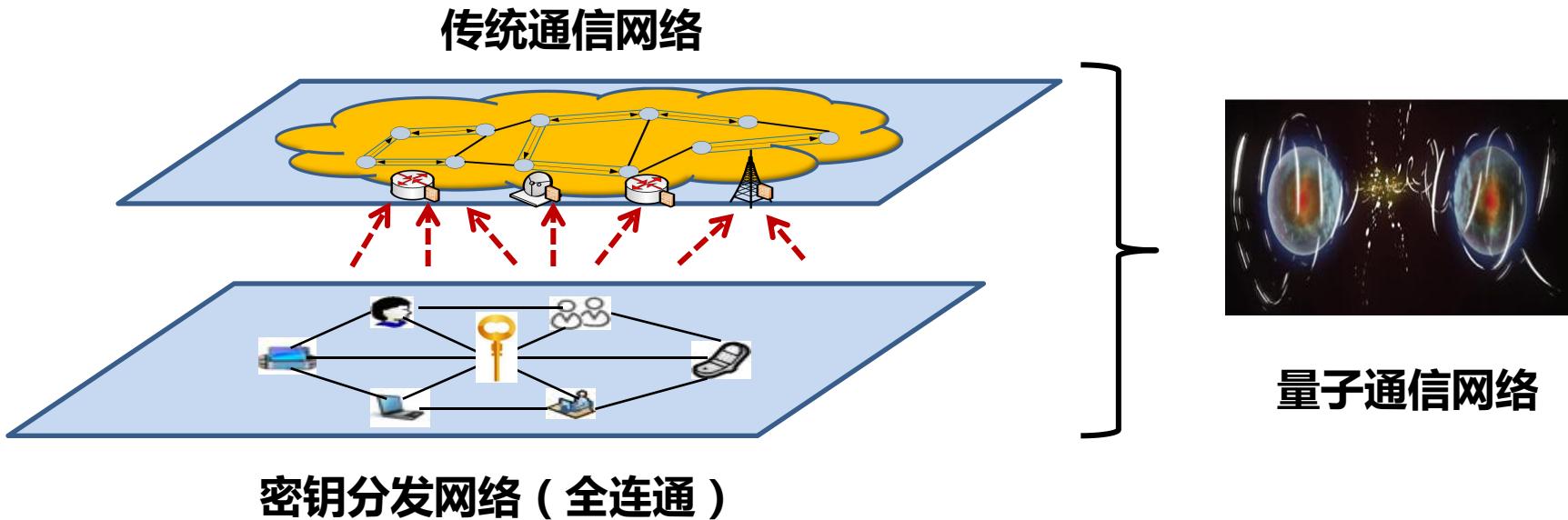


NFV安全需求分析



## □ 新型网络安全防护技术—量子通信网络安全

- 2016年7月，我国发射了世界首颗量子科学实验卫星，并在世界上首次实现卫星和地面之间的量子通信，**具有里程碑式的意义**。
- 面临挑战：量子通信无法脱离通信**实体验证**的信任基础；一次一密的秘钥协商和分发机制，带来了**通信效率、密钥存储和管理上的挑战**；密钥协商、数据通信均建立在**全联通的网络拓扑**上，在现实中难以构建此类网络。





## ◆ 研究背景

## ◆ 网络侧安全关键技术

## ◆ 数据侧安全关键技术

## ◆ 应用侧安全关键技术

## ◆ 一体化集成安全体系

## ◆ 主要工作进展



终端具备存储和  
计算能力

传输网络面临  
各类安全攻击

新型数据存储/处理技  
术（边缘计算/云存储）

在**传输、存储及处理**阶段全面保证**数据真实性、完整性和机密性**

## 数据传输安全

- 轻量级加密算法
- 多加密算法组合
- ...

## 数据存储安全

- 加密存储、访问控制、  
数据备份
- ...

## 数据处理安全

- 数据安全聚合
- 密文索引、密文计算
- 安全外包计算
- ...



## □ 密码学与数据安全

- 密码学研究：大多数都处于**理论阶段**，且关于未来密码学的研究成为当前研究热点（如**量子密码、后量子密码**）。
- 研究方向：平衡当下和未来密码学研究的比重，并且结合实际需求（**云计算、海量数据、物联网**等）研究可实用的安全加密算法。
- 数据传输、存储和处理不同的安全需求

	传输	存储	处理
数据状态	状态不变	状态不变	状态改变
数据时效	短时效	长时效	短时效



## □ 数据传输安全

- 考虑终端能力受限、高并发接入等需求，研究适用于网络传输的**轻量级加密算法以及完整性保护算法。**
- 其他安全技术：**多种密码算法组合**等

## □ 数据存储安全

- 研究**高效的数据加密算法**，在保证可用性的同时实现数据安全加密存储。相关技术包括**对称加密、同态、半同态加密**等。
- 研究**细粒度的访问控制机制**，保证灵活动态的数据安全访问与共享。相关技术包括**基于属性的访问控制策略**等。
- 其他安全技术：**数据完整性保护、灾后恢复、数据纠错**等

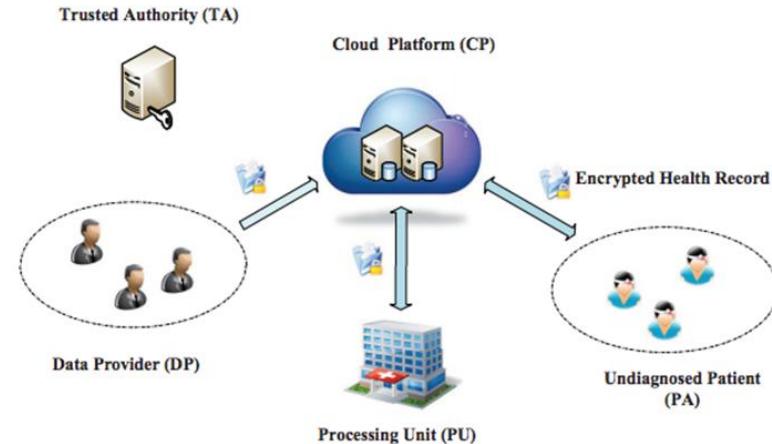


## □ 数据处理安全—密文计算方法

- 构造满足不可区分性安全的**密文计算算法**，设计**加密数据上的机器学习算法**，实现基于密文数据的直接计算操作并且保护数据的隐私。
- 其他安全技术：**多关键词加密数据搜索、安全外包计算**等



面向公有云的数据加密存储架构

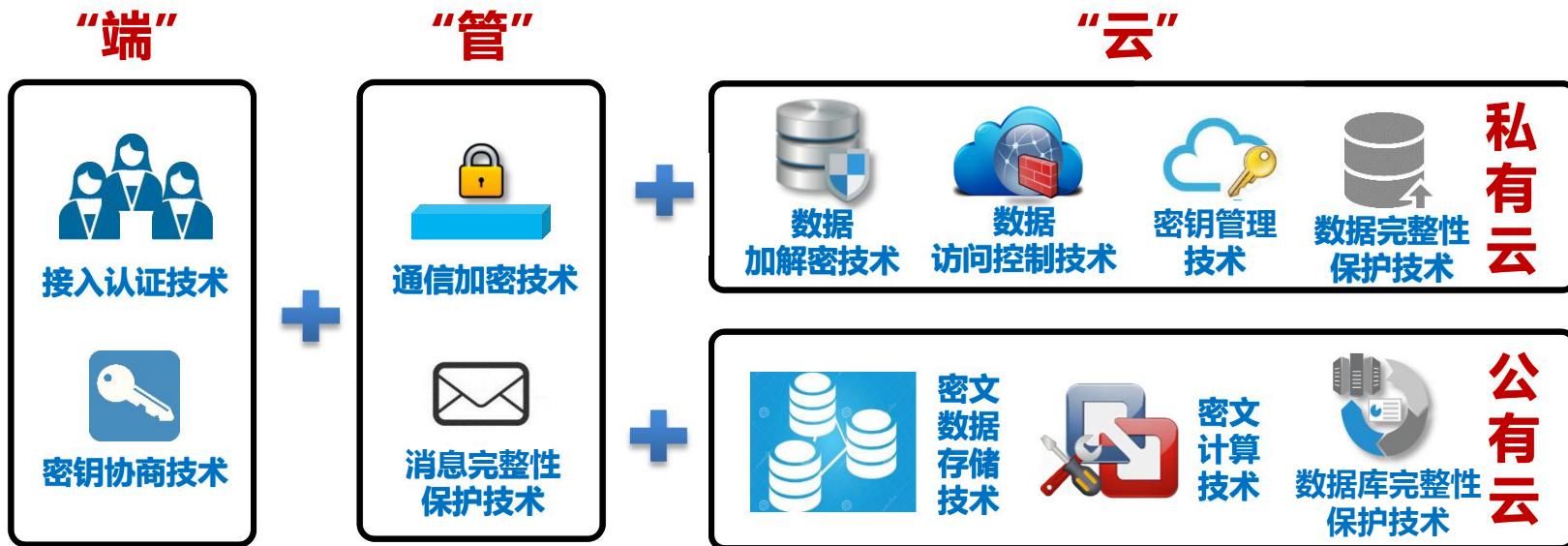


面向电子医疗云的密文计算框架



## □ 数据安全延伸—云安全体系架构

➤ 以数据侧安全机制为核心，结合**网络侧**和**应用侧安全机制**，构建“**云-管-端**”综合化安全体系架构，通过不同安全机制间的相互协同，实现云服务的全面安全防护。



”云-管-端“综合化安全体系架构



## 研究背景



## 网络侧安全关键技术



## 数据侧安全关键技术



## 应用侧安全关键技术



## 一体化集成安全体系



## 主要工作进展



多样化终端应用

不同应用协同服务

差异化安全策略

应用侧面临着来自终端、网络服务协同过程中各类安全威胁

终端/网络应用安全

- 身份认证、分区管理、恶意检测等
- 内容安全、舆情监控等
- 风险评估 ...

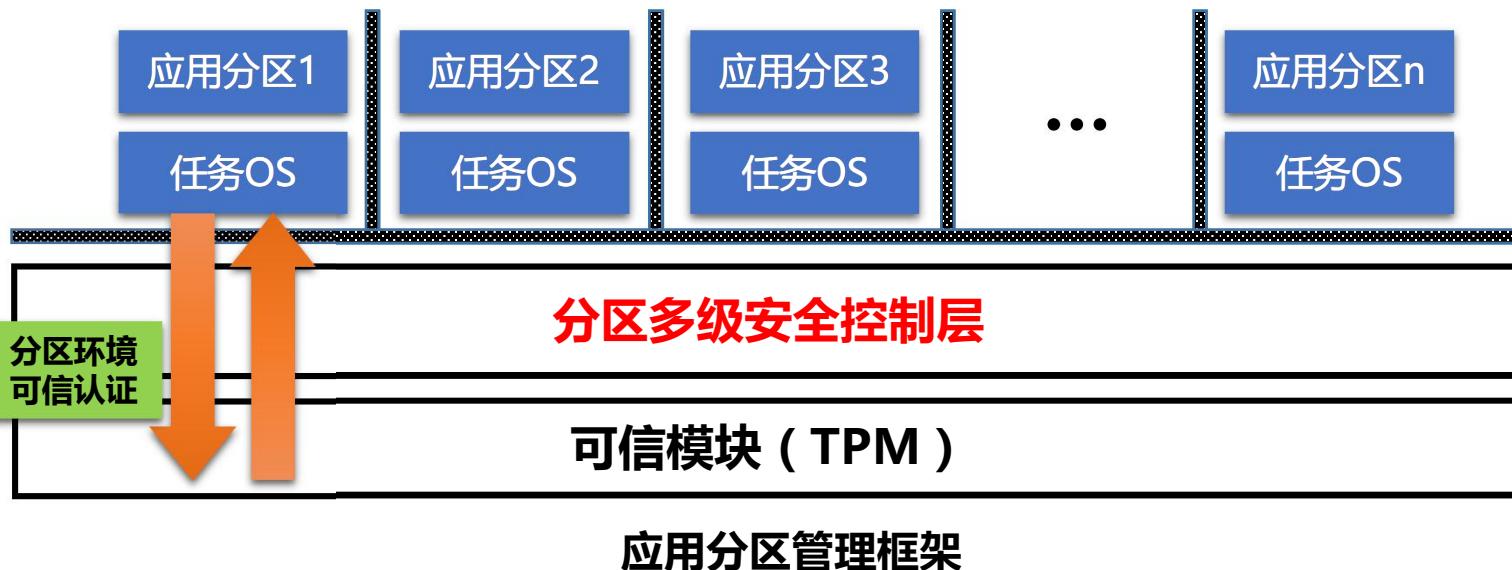
服务安全组合

- 服务安全组合方法
- 组合服务安全评估
- ...



## □ 智能设备应用安全

- **应用分区管理**：通过**可信验证机制**增强**分区的隔离性**，避免了终端应用易受恶意软件入侵而造成应用相互干扰的弊端。
- **恶意应用检测**：结合**静态分析**和**机器学习**对恶意行为进行精确建模，实现恶意应用的**高精度识别**。
- 其他安全技术：**漏洞修复**，**应用风险评估**等。





## □ 系统/应用层身份认证

- 传统身份认证：基于口令密码、用户生物认证；通过字符串匹配、模式识别等技术实现用户身份确认，**保证系统、应用资源安全。**
- 新型认证技术：基于用户行为、采用机器学习、数据挖掘等技术，实现**对用户身份的认证。**
- 与**网络层身份认证技术**相结合，提供**综合化身份防护体系。**



系统登录认证



应用登录认证



用户行为分析



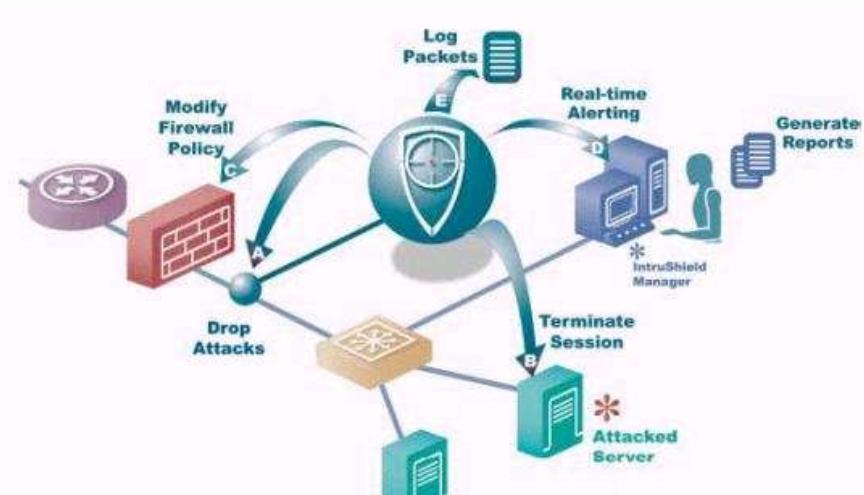
## □ 网络服务安全

- 内容安全：舆情监控等
- Web安全：Web客户/服务安全
- ...



舆情监控...

- 网络攻击防护：入侵检测等
- 服务可生存性

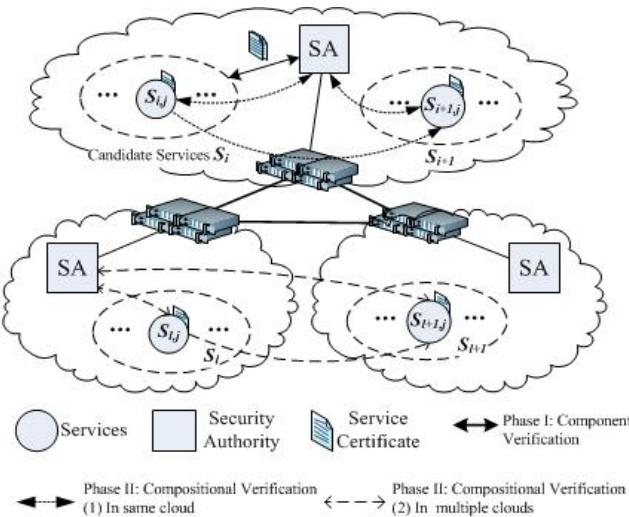


网络攻击防护

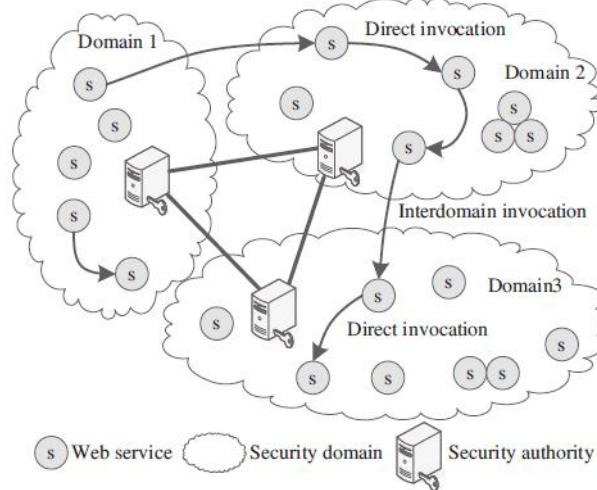


## □ 服务安全组合

- **服务安全组合**：**基于可证明安全模型的服务安全组合框架及方法**，实现服务组合过程安全性的**可分析和可验证**。
- **服务安全评估**：**基于信誉的网络服务评价模型与服务选择算法**，在确保评价的公平性的同时保证组合服务的**高可信度**。
- ...



服务安全组合框架



服务安全评估框架



## ◆ 研究背景

## ◆ 网络侧安全关键技术

## ◆ 数据侧安全关键技术

## ◆ 应用侧安全关键技术

## ◆ 一体化集成安全体系

## ◆ 主要工作进展



## 网络侧

- 终端假冒
- 非授权接入
- 网络攻击
- ...

## 数据侧

- 非授权访问
- 数据篡改
- 数据劫持
- ...

## 应用侧

- 安全策略不一致
- 信息泄露
- 应用漏洞
- ...

下一代网络系统面临着来自**网络、数据及应用**多个方面的安全挑战，采用单一的安全技术难以满足**终端，5G、SDN网络，云数据中心及各类网络服务**等的综合性安全需求。



APP重付漏洞门”



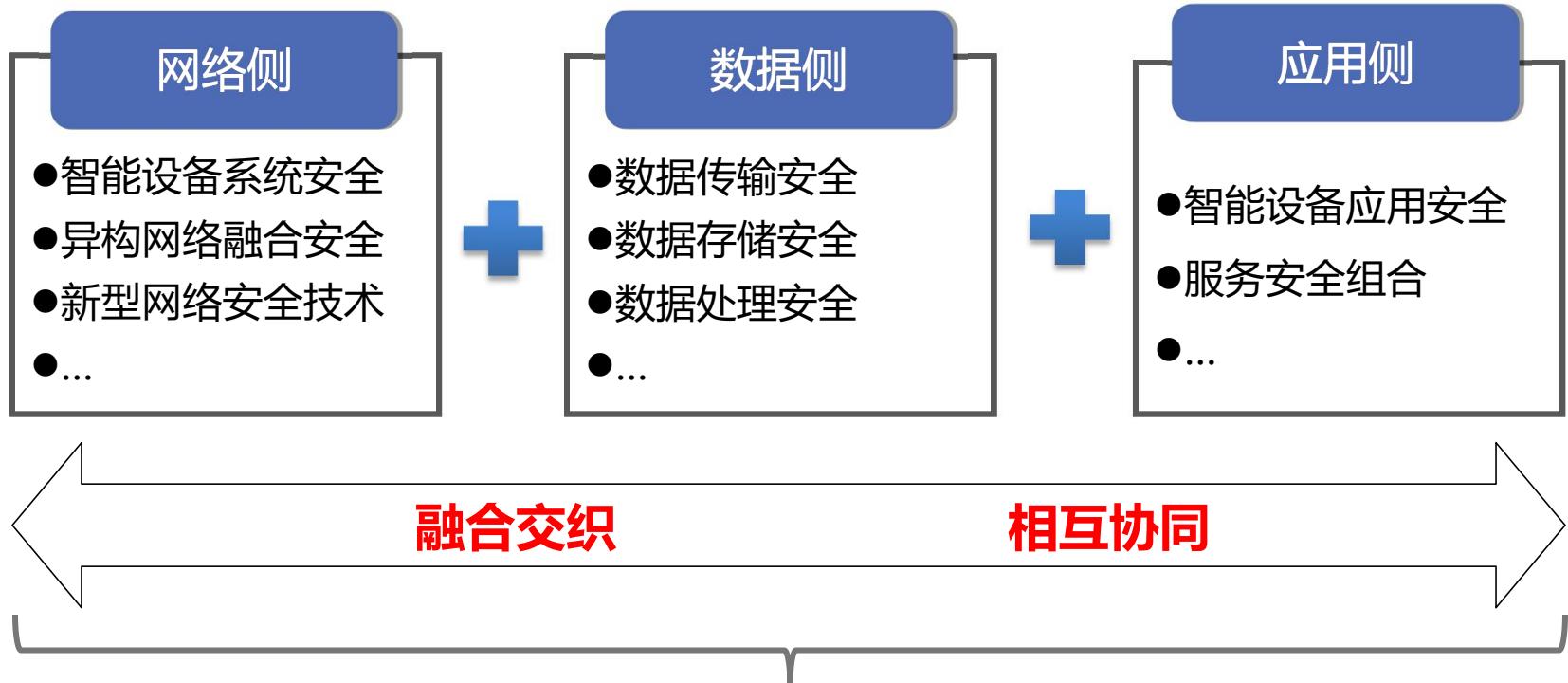
网络攻击  
(网络安全)



数据篡改  
(数据安全)



APP重应付  
(应用安全)



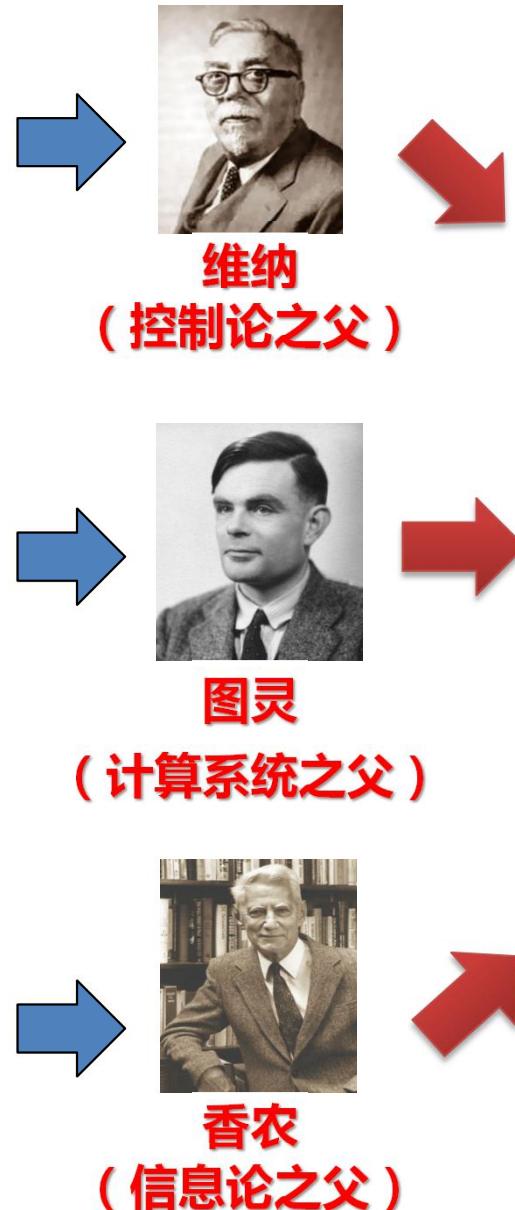
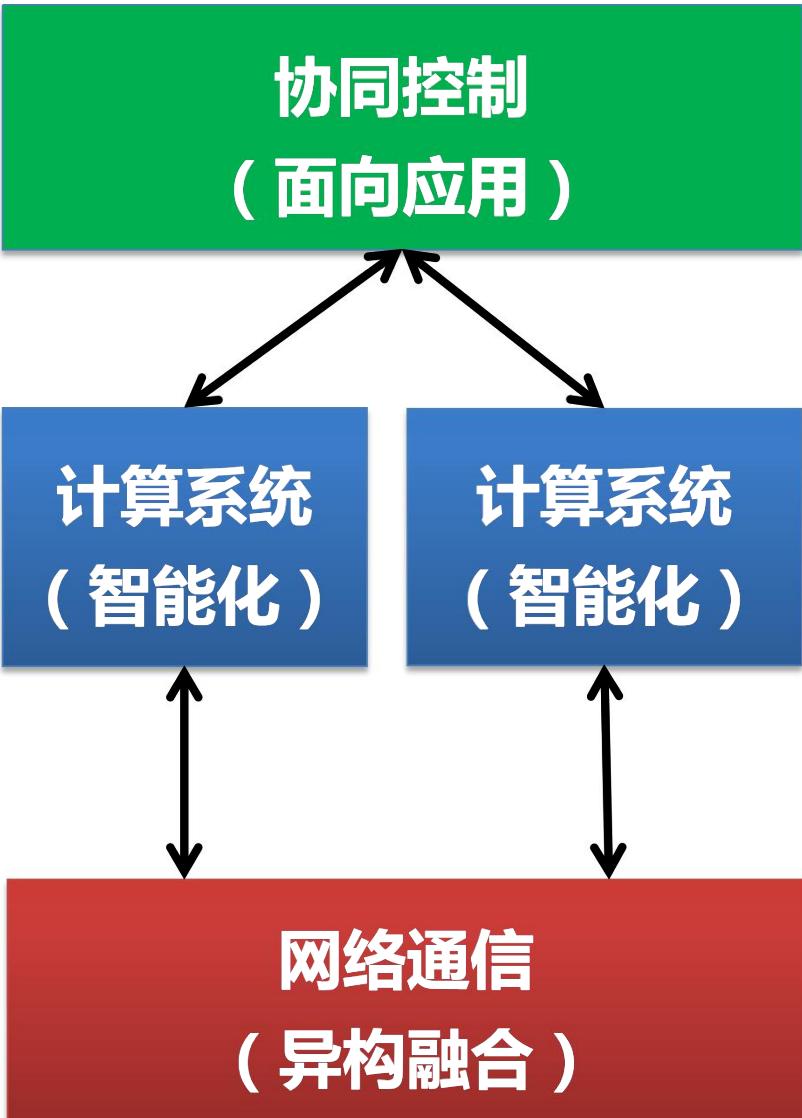
## “网络-数据-应用”一体化综合安全防护体系

下一代网络信息系统安全涉及网络、数据、应用等多个层次，构建**动态可扩展的“网络-数据-应用”一体化综合安全防护体系**，实现不同安全机制间的**协同防护**，共同保障下一代网络的安全。



设备及系统智能化、异构融合、面向应用是下一代网络信息系统的基本特征，为此，在下一代网络系统安全设计中，应该构建综合考虑网络、数据以及应用的一体化安全防护体系。





□ 安全是跨学  
科技术的融合  
。安全技术的  
研发与计算、  
通信、控制理  
论及技术的研  
究不可分割。



## ◆ 研究背景

## ◆ 网络侧安全关键技术

## ◆ 数据侧安全关键技术

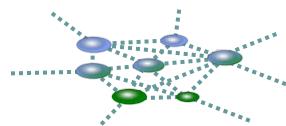
## ◆ 应用侧安全关键技术

## ◆ 一体化集成安全体系

## ◆ 主要工作进展



## 应用领域



5G网络安全



云安全



大数据安全



“互联网+”安全

...



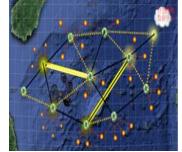
## 工程设计成果



安全移动终端



机载嵌入式安全平台



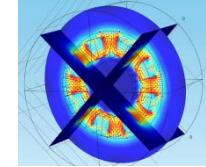
无人机安全组网



高并发加密服务器



云加密数据库



电磁云计算安全平台

无人系统协同控制

无人系统安全组网

智能系统安全设计

无线网络安全

云安全

一体化安全理论

安全外包计算与安全云平台

云数据加密结构与系统

高并发加密技术与系统

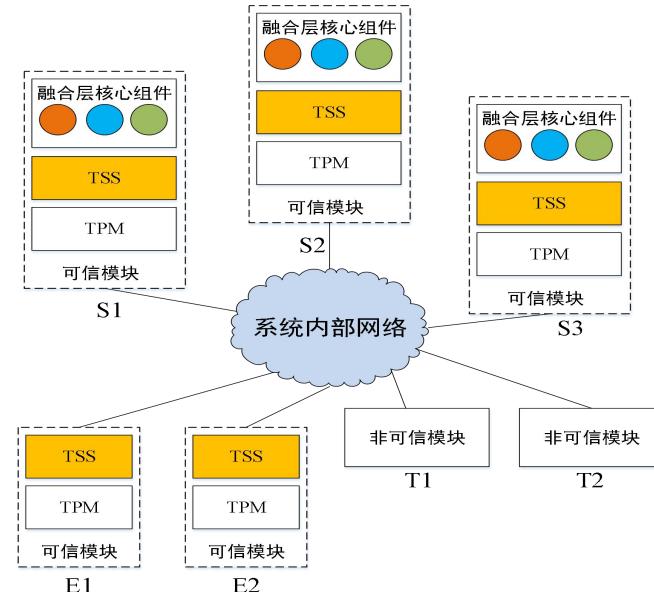
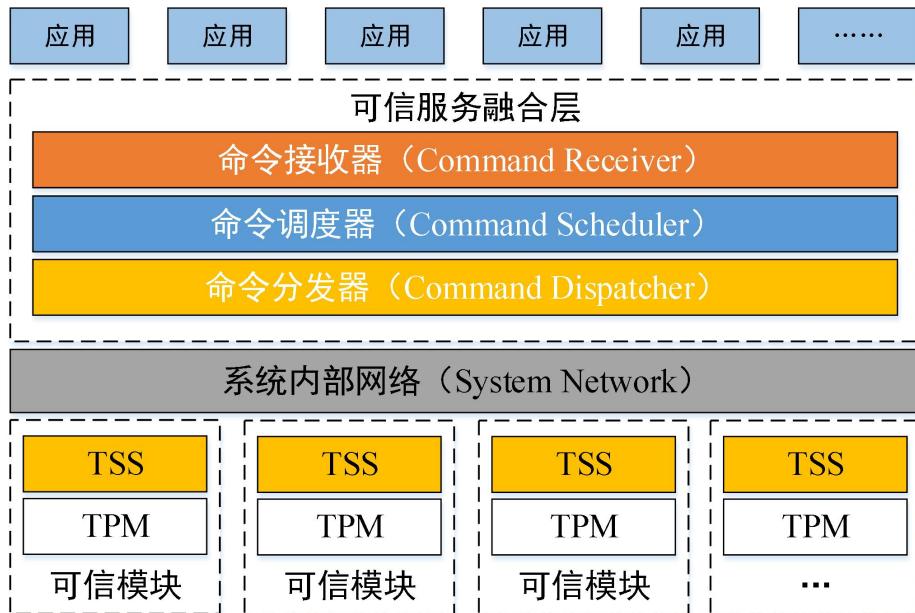






## □ 智能系统安全设计

- 可信服务融合架构：采用**可信根/可信服务融合、共享机制**，构建分布式信任体系，实现**信任由局部模块向系统整体的延伸**，解决集中式信任链过长的问题，确保**系统整体的安全性和可靠性**。
- 其他安全技术研究：平台运行时实时监控技术等。





## ➤ 具体应用—机载嵌入式安全平台

基于所研究的**基于TPM的可信安全平台**关键技术，联合**中航工业631所**设计并实现了**机载嵌入式安全平台**。该平台综合考虑**安全性和可靠性（Safety&Security）**，已实际**部署于某型号航空嵌入式系统**中，未来还可应用于**宽体客机的信息安全防护系统**。





## □ 无人智能设备安全攻击

- 针对**无人机系统服务缺陷**，**挖掘未知安全漏洞**，迫使**系统崩溃**，**迫降无人机**。
- 针对**无人机网络侧安全缺陷**，进行**恶意数据无线注入**，**劫持无人机**。

### 2017年春晚演出DOBBY无人机攻击



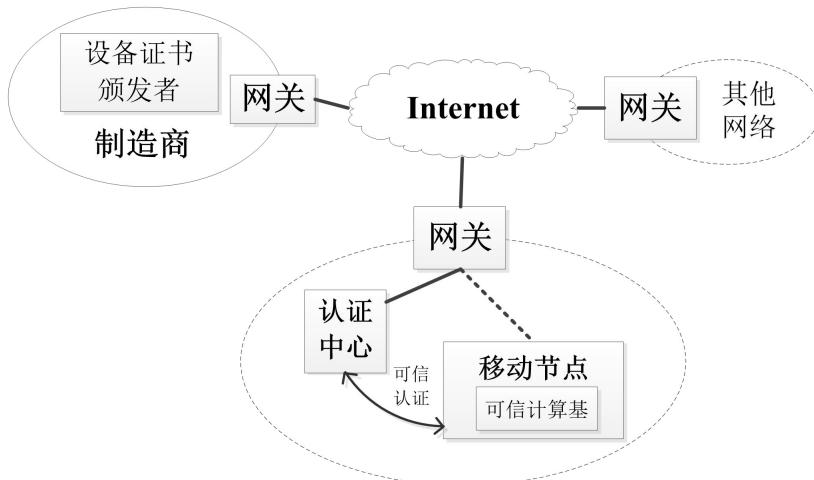
```
Zmap
扫描(a) 工具(t) 配置(p) 帮助(h)
目标: 192.168.1.1
命令: nmap -T4 -A -v 192.168.1.1
主机 服务 Nmap输出 端口/主机 托扑 主机明细 扫描
操作系统 主机 v
nmap -T4 -A -v 192.168.1.1

Starting Nmap 7.31 ( https://nmap.org ) at 2017-03-08 16:20 CST
NSE: Loaded 142 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:20
Completed NSE at 16:20, 0.00s elapsed
Initiating NSE at 16:20
Completed NSE at 16:20, 0.00s elapsed
Initiating ARP Ping Scan at 16:20
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 16:20, 0.05s elapsed (1 total hosts)
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers
Initiating SYN Stealth Scan at 16:20
Scanning 192.168.1.1 [1000 ports]
Discovered open port 21/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 8080/tcp on 192.168.1.1
Discovered open port 5555/tcp on 192.168.1.1
Completed SYN Stealth Scan at 16:20, 0.32s elapsed (1000 total ports)
Initiating Service scan at 16:20
```

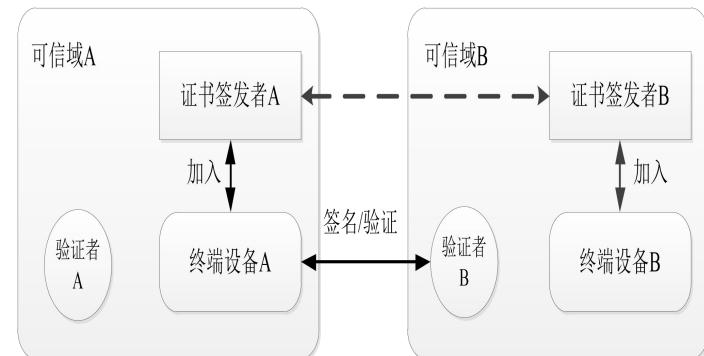


## □ 无人系统安全组网

- “端-网”可信连接技术：设计“端-网”可信连接架构，发明了网络身份认证与系统安全验证相结合的可信连接(TNC)模型，弥补了传统身份认证缺乏系统安全验证的缺陷，增强了网络连接的安全性。



移动终端设备认证方法

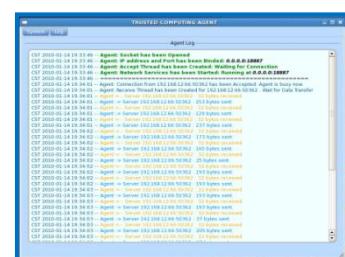
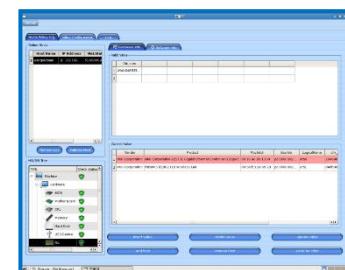
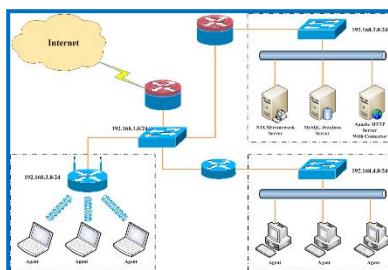


跨网安全验证方法



## ➤ 可信网络连接模型

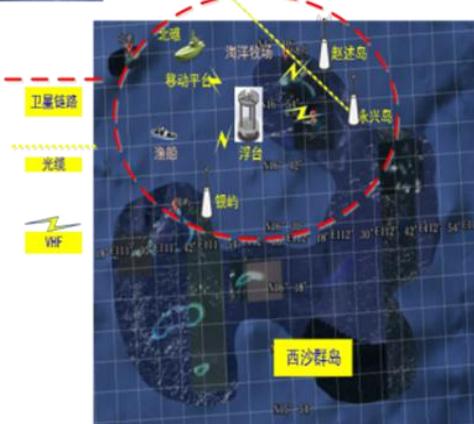
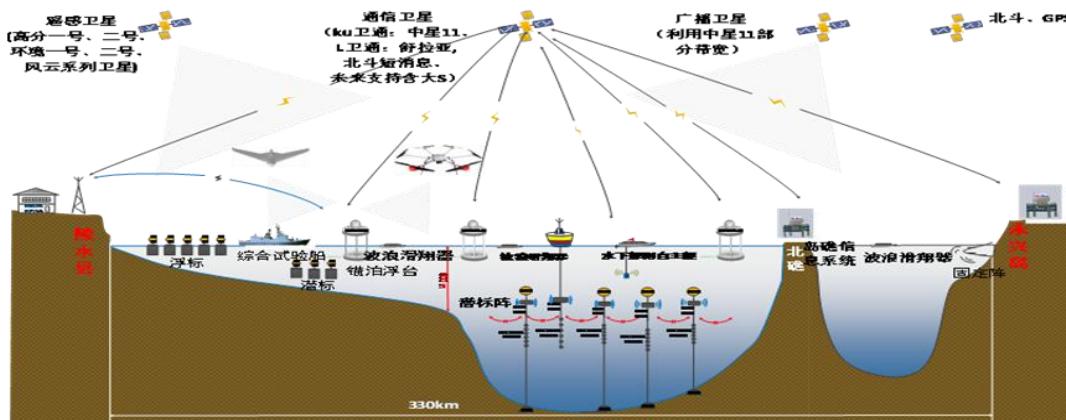
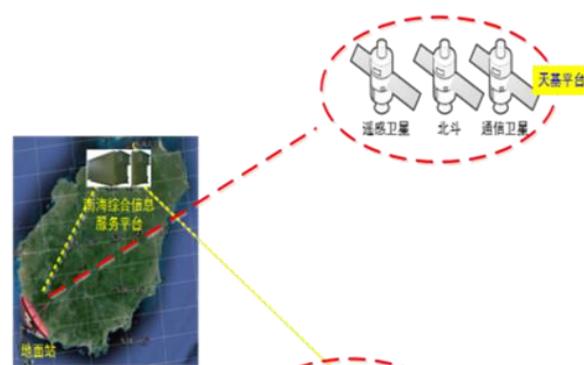
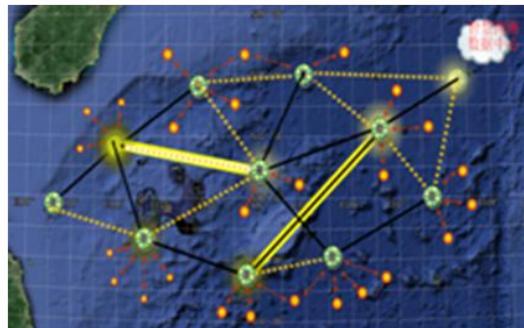
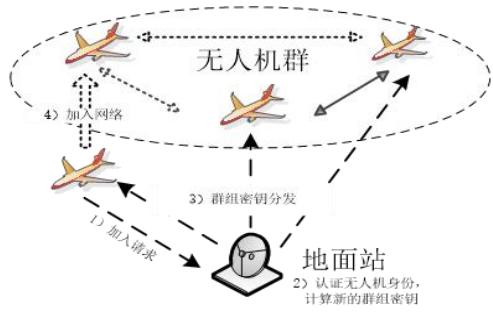
该模型被认为是首个通用可组合的可信网络连接模型，弥补了可信计算联盟（TCG）网络连接方案中用户认证和平台校验缺少安全关联的缺陷，相关技术目前已被纳入国家标准。





## ➤ 具体应用—无人机安全组网系统

在可信网络连接关键技术支撑下，设计了首个**无人机安全组网系统**，  
系统正准备进行安全测试，对空天地海一体化安全网络建设具有重要意义。





## □ 无线网络基础设施安全性分析

- 对我国高校无线网络基础设施进行**安全性分析与评估**，发现存在多方面的**安全漏洞**与**严重安全隐患**，威胁人身与财产安全，泄露JS科研机密，危害公共安全与社会稳定，甚至威胁国家安全。



### 测试内容

校园网传输账号密码方式测试

上网数据是否加密测试

无感知认证测试

邮箱登陆测试

假路由测试

7个城市 8463.6公里 360小时 19所知名高校 112个口令获取 300G数据量截获

学科攻击类型	敏感信息泄露										主动攻击						伪装欺骗			被动攻击			关链信息窃听							
	个人 信息 泄露	公事 信息 泄露	内网设备 数据窃取	位置 信息 泄露	数据 篡改 分析	口令 破解	非法 注入	Cookie 伪造	MAC 伪装	DNS 劫持	ARP 欺骗	青 蜂 攻击	数据 报文 篡改	应用 劫持	暴力 破解	漫 游 攻击	社 会 工程	恶意 同行 监听	劫 持 端口 监听	网 络 信 息 窃 听										
	个人 信息 泄露	公事 信息 泄露	内网设备 数据窃取	位置 信息 泄露	数据 篡改 分析	口令 破解	非法 注入	Cookie 伪造	MAC 伪装	DNS 劫持	ARP 欺骗	青 蜂 攻击	数据 报文 篡改	应用 劫持	暴力 破解	漫 游 攻击	社 会 工程	恶意 同行 监听	劫 持 端口 监听	网 络 信 息 窃 听										
清华大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
北京大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
北京航空航天大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
北京邮电大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
北京理工大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
天津大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
南开大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
燕京理工学院	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
首都经济贸易大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
首都师范大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
中国科学院大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	(可以实现)
浙江大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
复旦大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
南京大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
上海交通大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
西安交通大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	(可以实现)
西北工业大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
西北农林科技大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
西安理工大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
西安电子科技大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
陕西师范大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
陕西科技大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
陕西理工大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
陕西师范大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
陕西科技大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
陕西理工大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
陕西理工大学	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y



## □ 无人系统协同控制

### ➤ 群体智能模型

- **核心思想**: 智能源于社会性的相互作用
- **主要特征** : 个体感知有限, 行为简单 ; 受相邻个体影响、交互、协作 ; 无集中控制、分布式 ; 具有自组织性、涌现性

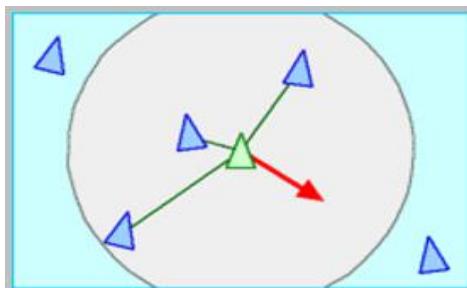




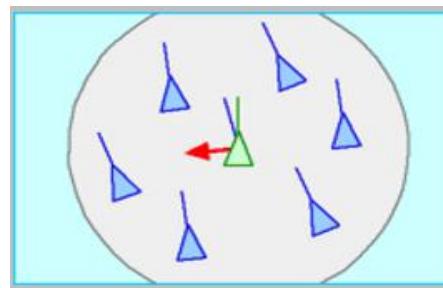
## □ 无人系统协同控制

### ➤ Reynolds's Boids 模型（经典模型）

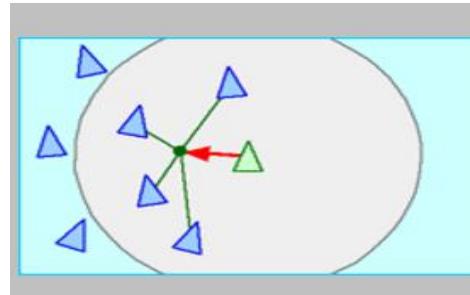
- 基于简单的三个规则模拟鸟群、鱼群等的飞行：分离（与相邻群体保持分开）、对齐（朝向相邻群体的平均方向）、粘合（朝向相邻群体的平均位置）。



**Separation:**  
steer to avoid  
crowding local  
flockmates



**Alignment:**  
steer towards  
the average  
heading of  
local  
flockmates



**Cohesion:**  
steer to move  
toward the  
average  
position of  
local  
flockmates



## □ 无人系统协同控制

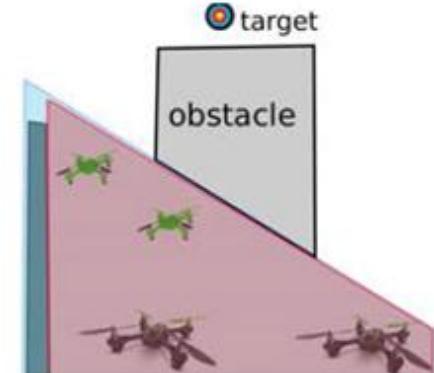
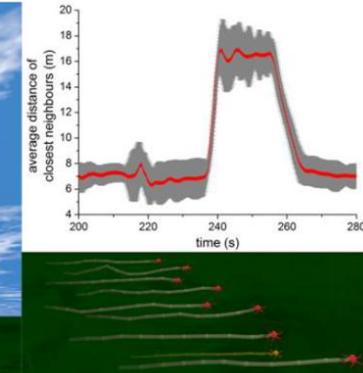
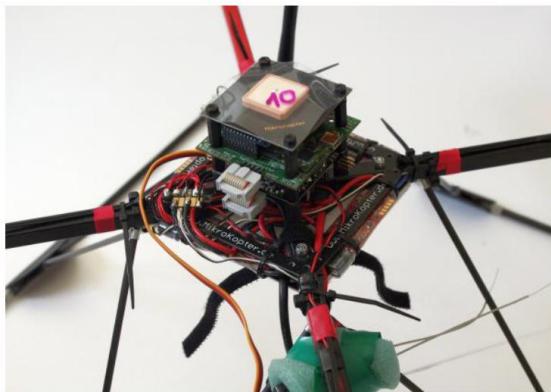
### ➤ 典型群体智能算法

- 粒子群算法 (Particle Swarm Optimization, PSO) : 模拟模拟鸟群觅食现象
- 蚁群算法 (Ant Colony Optimization, ACO) : 借鉴蚂蚁觅食通信原理
- 人工蜂群算法 (Artificial Bee Colony, ABC)
- 细菌觅食优化算法 (Bacterial Foraging Optimization, BFO)
- 人工免疫系统 (Artificial Immune System)
- . . .



## □ 典型应用

- 基于Boids模型的无人机组队飞行 (2014)
  - 实现了分布式通信、碰撞避免；可协同控制10架无人机；对噪声、延时、通信范围有一定的容忍度。
- 分布式多机器人组队控制 (MIT, 2016)
  - 实现了在2D, 3D空间内在静态、动态障碍物下协同飞行。





## 应用领域



5G网络安全



云安全



大数据安全



“互联网+”安全

## 工程设计成果



安全移动终端



机载嵌入式安全平台



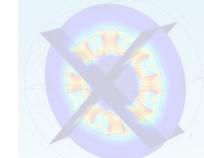
无人机安全组网



高并发加密服务器



云加密数据库



电磁云计算安全平台

无人系统协同控制

无人系统安全组网

智能系统安全设计

无线  
网络安全

云安全

一体化安全理论

安全云平台

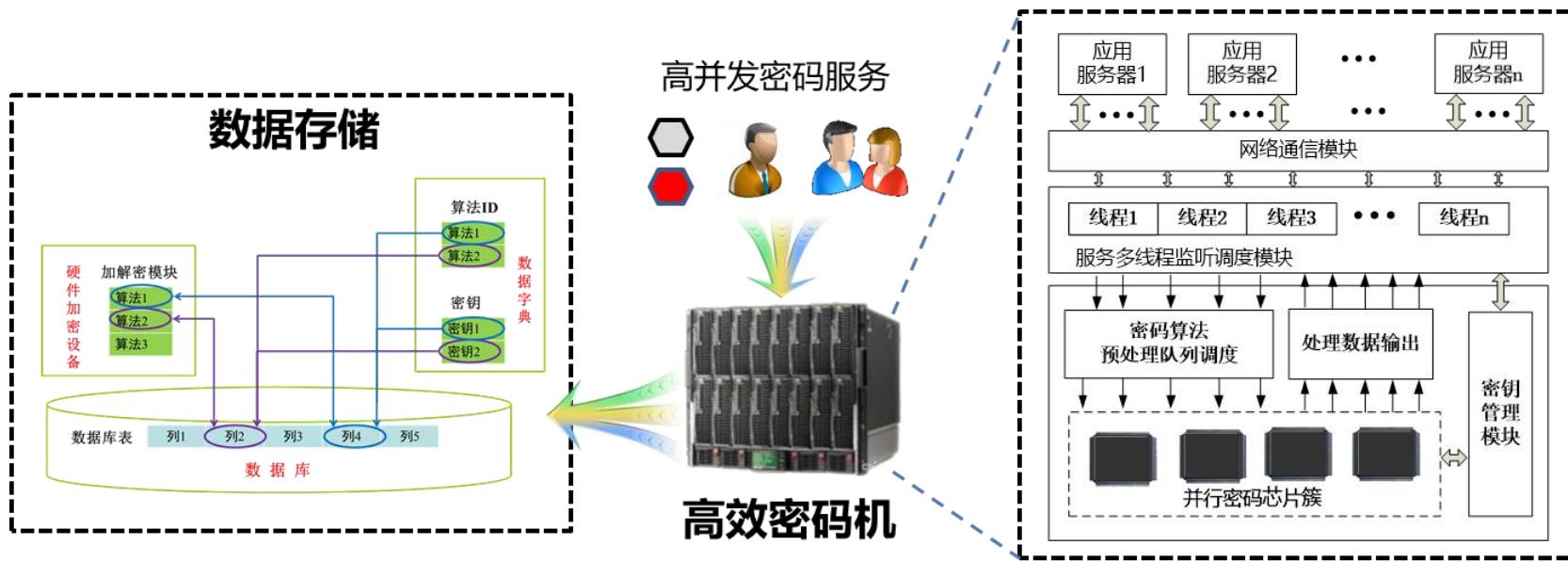
云数据安全

高并发加密  
技术与系统



## □ 高并发加密技术与系统

➤ 提出了“服务状态跨层跟随”的高性能密码服务计算架构，发明了可迁移的海量密钥保护方法和密码芯片级的多算法/多密钥/多数据流随机交叉加解密方法，实现了高并发的数据安全处理，保证了多源异构数据的机密性。





## ➤ 具体应用—高性能综合密码服务系统

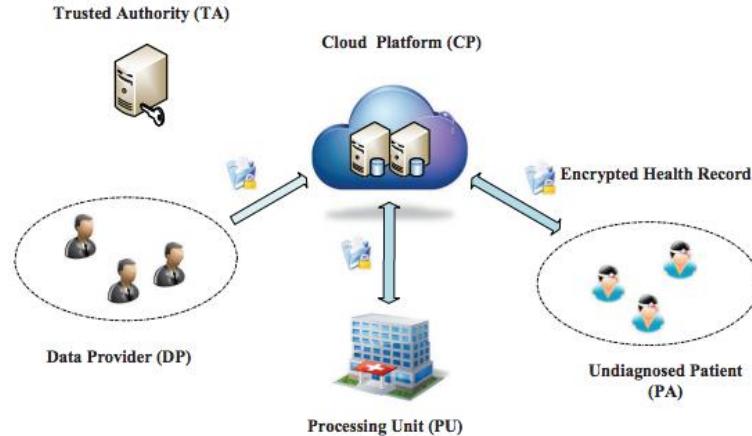
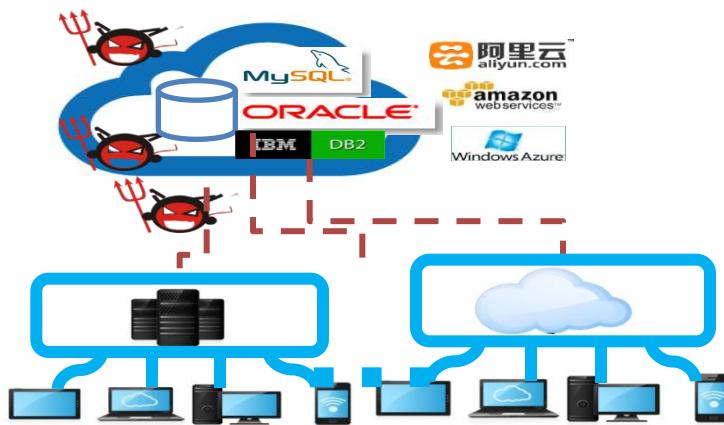
基于上述技术所研制的**高性能综合密码服务系统(SJJ1405、SRJ1310和SJJ1330)**被国家密码管理局批准为商用密码产品，**并在国家密码管理局的综合测评中性能指标排名第一**，具有广泛的应用前景。

对比项	本发明 (SJJ1405)	江南 天安	山东 渔翁	对比项	本发明 (SRJ1310)	江南天 安	对比项	本发明 (SJJ1405)	山东 渔翁
SM4加解密	50Gbps	9Gbps	8.7Gbps	SM4加密	23Gbps	7Gbps	SM2密钥生成	21.7万对/秒	2.2万对/秒
SM2性能	8.7万次/秒	3万次/秒	1.3万次/秒	SM4解密	23Gbps	7.8Gbps	SM2签名	17万次/秒	14万次/秒
在线并发密钥量	3.96亿	NA	NA	网银交易	26万笔/秒	10万笔/秒	SM2验签	7万次/秒	4.5万次/秒
				磁条卡交易	15.5万笔/秒	7万笔/秒	网银签发	9.4万次/秒	1万次/秒
				IC卡交易	10.8笔/秒	6.8万笔/秒			



## □ 数据加密存储、传输与处理

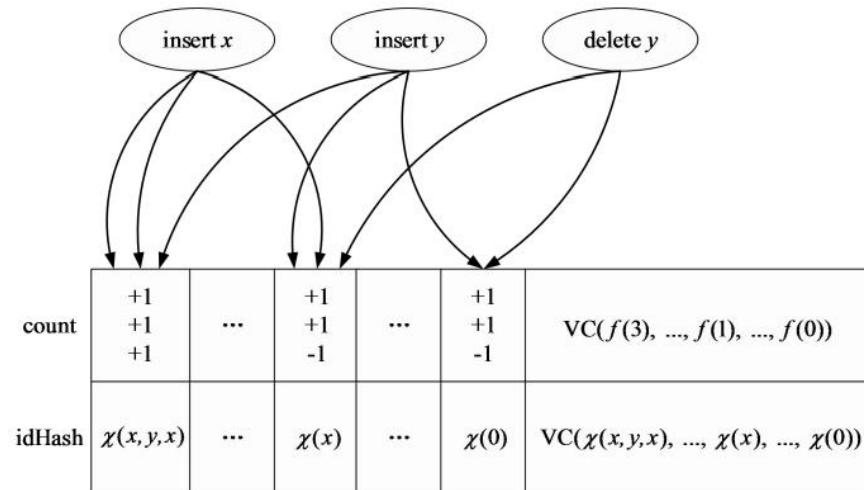
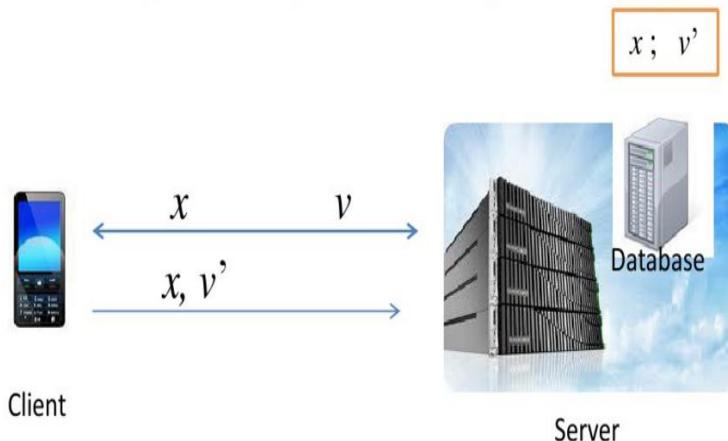
- **数据加密存储**：发明了**基于明文索引的密钥管理方法**及**自适应可定制的数据库列分级加密技术**，保证数据机密性的同时兼顾数据可用性。
- **数据安全传输**：结合网络层安全传输技术，采用**并行加密传输技术**，提高**密文数据的传输效率**。
- **数据安全处理**：提出了**基于半同态的数据安全计算方法**，实现基于密文数据的直接操作（聚合、计算等），保护了**数据的机密性和隐私性**。





## □ 数据完整性验证

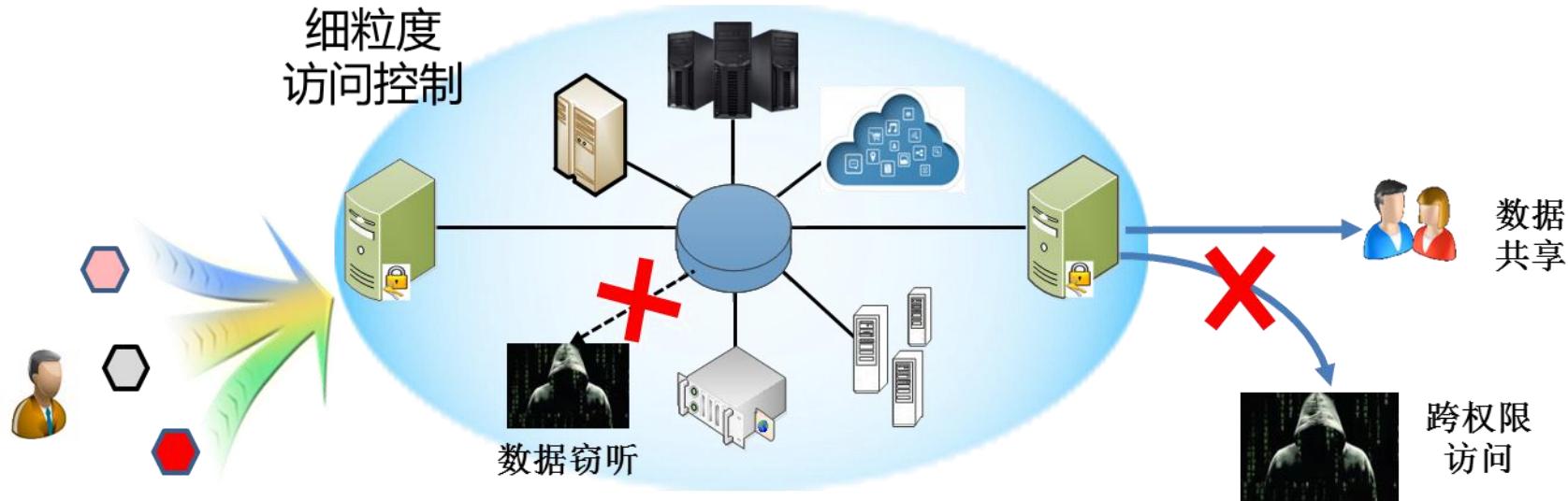
- 提出了**云计算下大数据库的可验证更新方案**，解决了**动态大数据库中可公开验证性与自动更新攻击之间的不兼容问题**。
- 提出了**可验证的递增更新数据库的概念**，解决了**动态大数据库中数据频繁更新操作计算效率低下的问题**。





## □ 数据隐私保护

- **数据加密存储/传输/处理**：**加密数据的存储、计算及处理**在保证机密性同时也**保护了用户数据的隐私性**。
- **数据安全共享**：设计**基于属性的细粒度的访问控制机制**，保护**用户数据隐私性**的同时，实现了**灵活动态的数据安全访问与共享**。





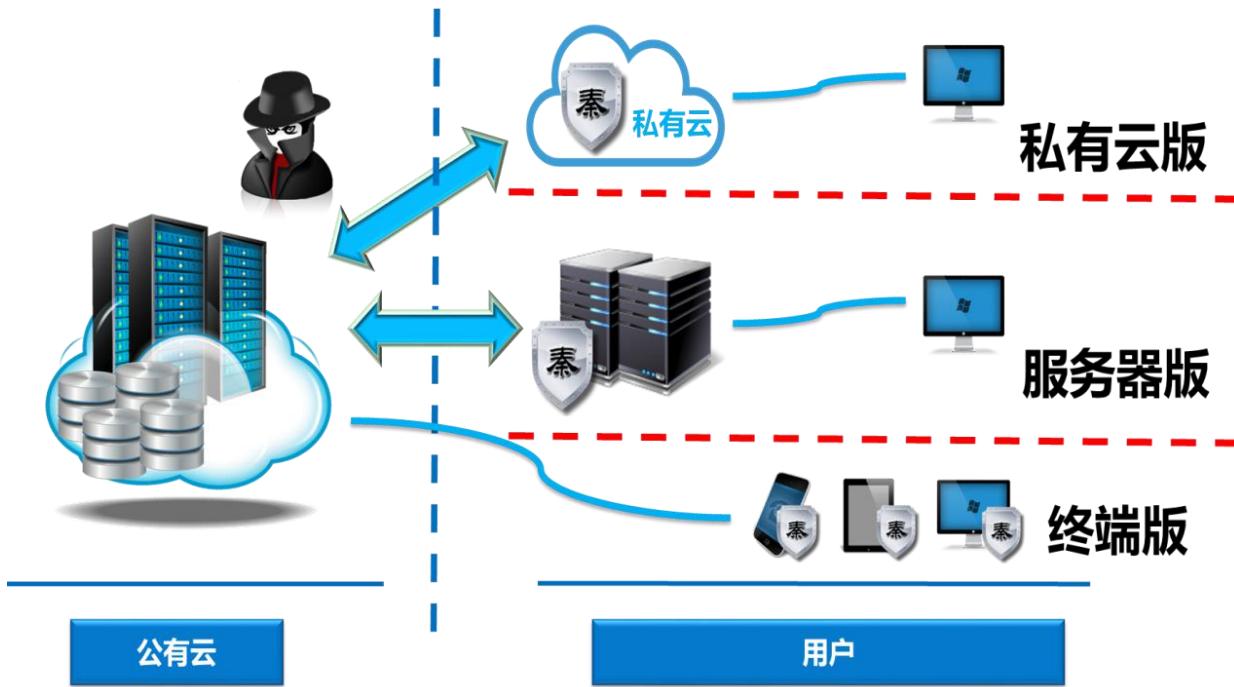
## ➤ 具体应用—秦盾云加密数据库

相较麻省理工学院MIT的CryptDB数据库，所提出的云加密数据库技术在不降低安全性的前提下采用了一次加密模式，支持密文数据的完整性验证，实现了可定制列数据分级加密、细粒度访问控制及并发密文数据的有效更新，提高了系统的实用性。

数据库方案	支持关系数据操作	密文存储	密钥本地化管理	列级加密定制	数据共享	完整性验证
关系型数据库(RDS)	√	✗	---	---	---	---
MIT CryptDB	√	√	√	✗	✗	✗
“秦盾”(QinCloudDB)	√	√	√	√	√	√



基于所研究的**数据加密参考结构**等关键技术，自主研发的“**秦盾**”**云加密数据库系统**。作为基础软件安全系统，获得了第十八届中国科协年会全国科技工作者创新创业大赛“**金奖**”(16/1800+)，“**最佳商业投资价值奖**”(2/1800+)。





“秦盾”数据库系统参加了**第二届军民融合发展高技术成果展**，新华社报道中被认为在军民融合领域拥有广阔应用前景。



# 云安全关键技术（二）



权威发布 / 正文

## 习近平参观军民融合发展高技术成果展

来源：新华社 作者：张晓松 杨维汉 责任编辑：高丽萍 2016-10-19 18:21



习近平在参观第二届军民融合发展高技术成果展时强调

加快形成军民深度发展格局 为实现中国梦强军梦作出新的更大的贡献

李克强张德江俞正声刘云山王岐山张高丽参观展览

中共中央总书记、国家主席、中央军委主席习近平19日在北京参观第二届军民融合发展高技术成果展。他强调，军民融合是国家战略，关乎国家安全和发展全局，既是兴国之举，又是强军之策。军民融合不断取得阶段性成果，呈现出加快发展良好态势。要继续推动体制机制改革创新，从需求侧、供给侧同步发力，从组织管理、工作运行、政策制度方面系统推进，继续把军民融合发展这篇大文章做实，加快形成军民深度发展格局，切实打造军民融合的龙头工程、精品工程，为实现中国梦强军梦作出新的更大的贡献。

中共中央政治局常委李克强、张德江、俞正声、刘云山、王岐山、张高丽分别参观展览。

上午9时30分，习近平来到中国人民解放军装甲兵工程学院，走进展厅参观展览。展览由中央军委装备发展部、教育部、工业和信息化部、国防科工局、全国工商联联合举办，以“全面落实军民融合国家战略、全面推进军民深度融合发展”为主题，共分为科技创新区、竞争活力区、基础保障区、信息发布区、大型实装展示区等5个展区，通过高技术产品、高新技术成果等，全面系统展示党的十八大以来军民融合发展的阶段性成果。

技术先进的北斗导航卫星、水下机器人，可替代进口器件的精密光学仪器，军民通用计算机和射频集成电路；  
在军民融合领域拥有广阔应用前景的整体精密铸造技术、碳纤维及其复合材料核心技术、云数据加密技术；高效便捷的混合动力新能源电站，拥有自主知识产权的大型激光3D打印机，整齐排列的无人机、无人舟艇等大型装备……  
一件件实物、一个个模型、一段段精彩视频，吸引了习近平等领导同志的目光。他们不时停下脚步仔细观看，认真听取讲解，并详细询问有关情况。

在京中共中央政治局委员、中央书记处书记，国务委员以及中央军委委员参观了展览。



## □ 一体化安全云平台

- 提出了贯穿云计算架构的**一体化云安全技术支撑体系**，涉及**云平台可信接入技术**；**数据库加密技术**；**虚拟机安全管理技术**，**网络安全管理**等不同的安全机制。
- 通过不同层次安全机制的协同，构建**一体化安全云平台**。

一体化云安全技术支撑体系

SaaS



虚拟机安全态势监控技术



网络设备状态安全监控技术



文件安全存储技术



虚拟机安全管理技术



云平台网络安全管理技术



云平台快速部署技术

PaaS



数据库加密技术



云应用安全API

IaaS

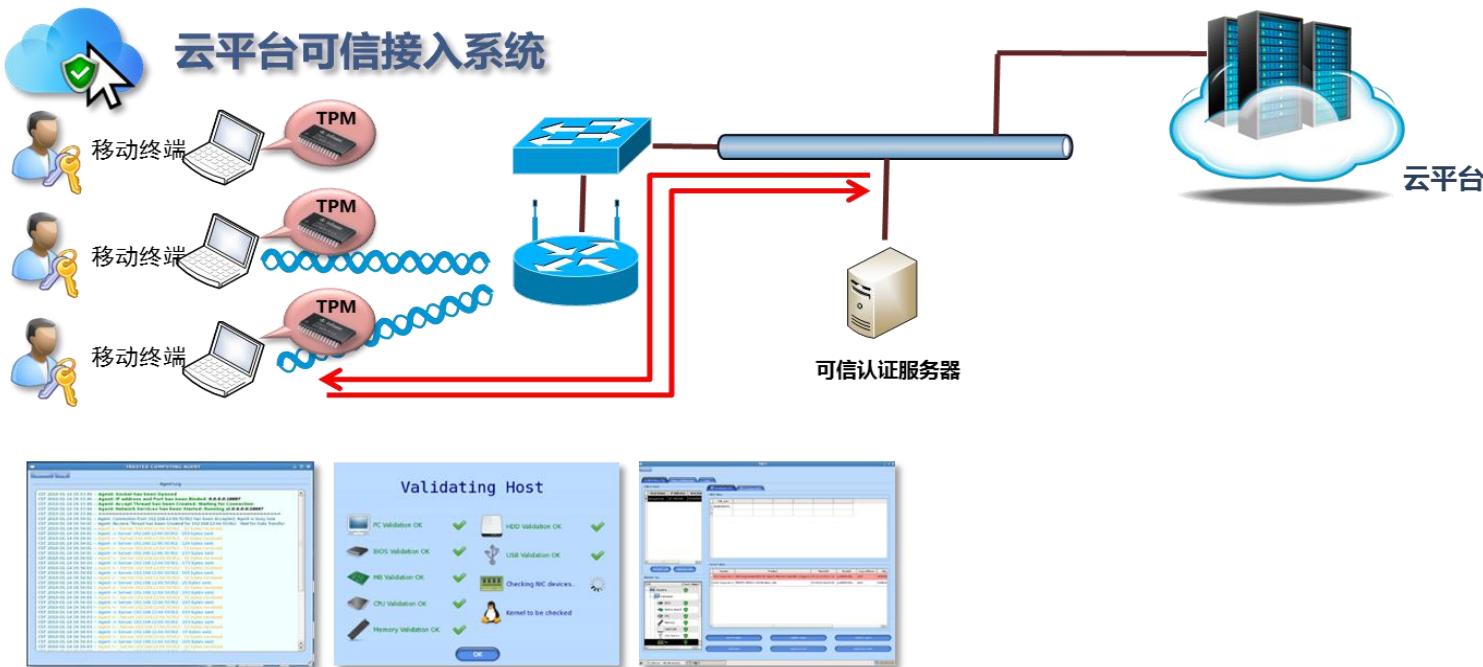


云平台可信接入技术



## □ 云平台可信接入技术

- 基于**TPM芯片**，提供**结合用户口令与设备物性特征的接入方式**，避免了单一口令容易泄露问题；对设备物性特征的验证实现了对用户设备的严格管控，大大降低了非法设备接入的风险。





## □ 数据库加密技术

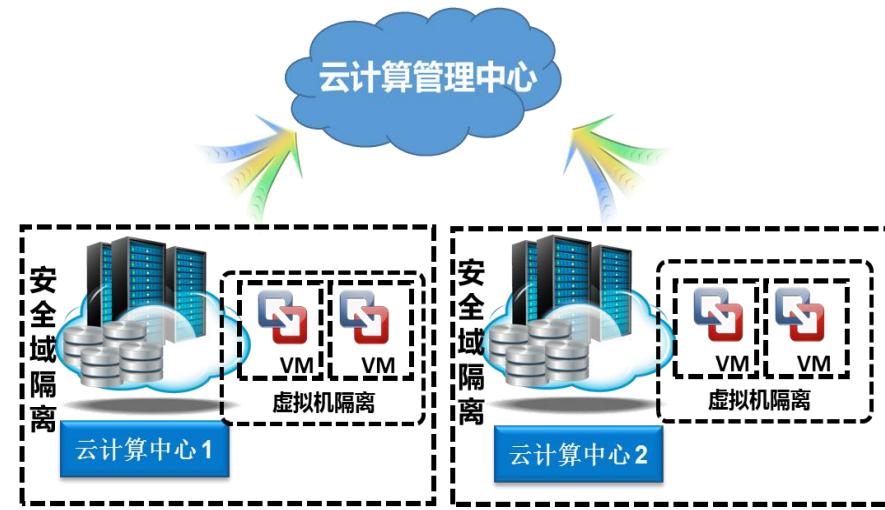
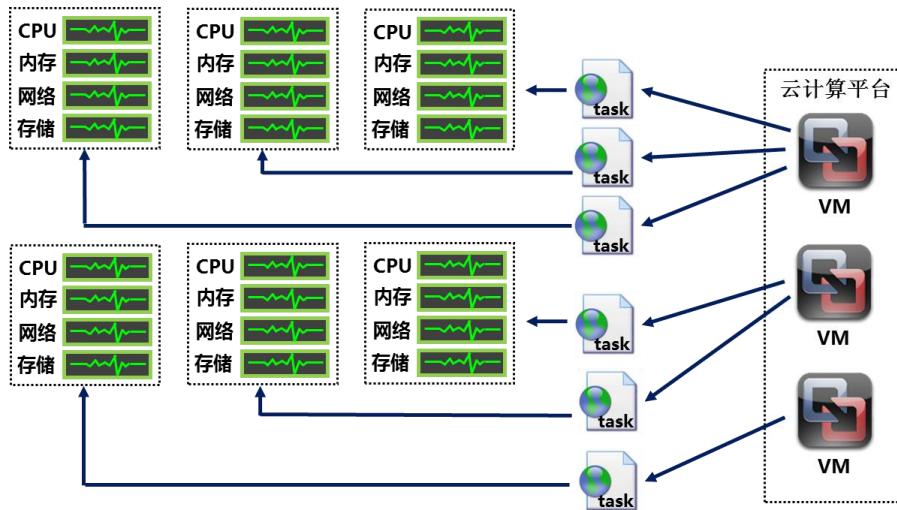
- “秦盾”数据库核心技术，为用户和应用程序提供加密数据库服务。包括**加密检索、加密数据上传、安全数据操作**等。
- 采用**全透明运行模式**，轻松使用的同时享受全面的数据安全防护，支持面向终端、服务器、私有云等场景的部署方式。





## □ 虚拟机安全管理技术

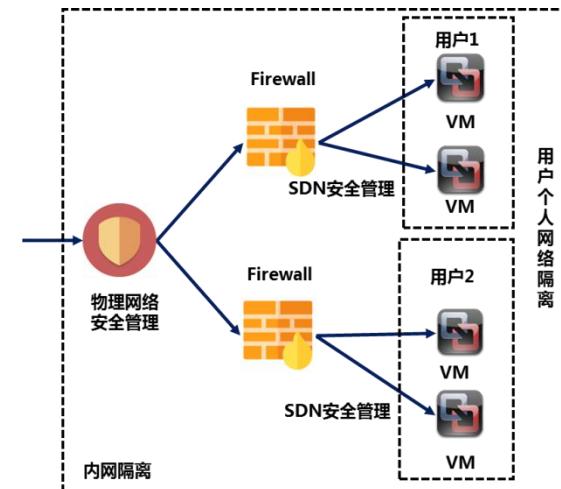
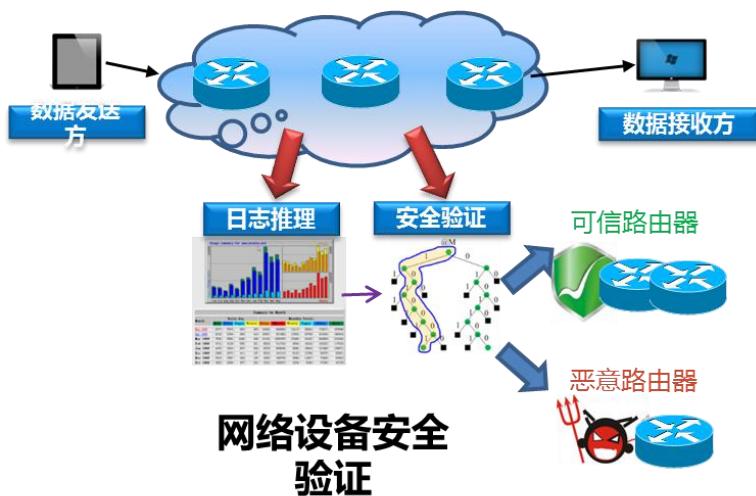
- **任务级虚拟机运行时监控技术**：提供面向虚拟机内任务的运行时监控，任务运行时状态数据分析挖掘服务，及时发现异常行为，根据灵活的监控策略终止或暂停有危害的任务；
- **分域管理，安全域隔离**：依据安全级严格控制数据流和控制流；权限分级，防止操作权限失控，保证系统全稳定运行。





## □ 网络安全管理技术

- **网络通信设备可信验证技术**：利用机器学习方法，通过对日志记录分析，对网络中各类通信设备进行安全验证。
- **网络安全管理系统**：针对各类网络攻击，构建面向用户的防火墙服务、多维度的网络攻击防护等多种防护手段，增强云平台所属网络的安全性。





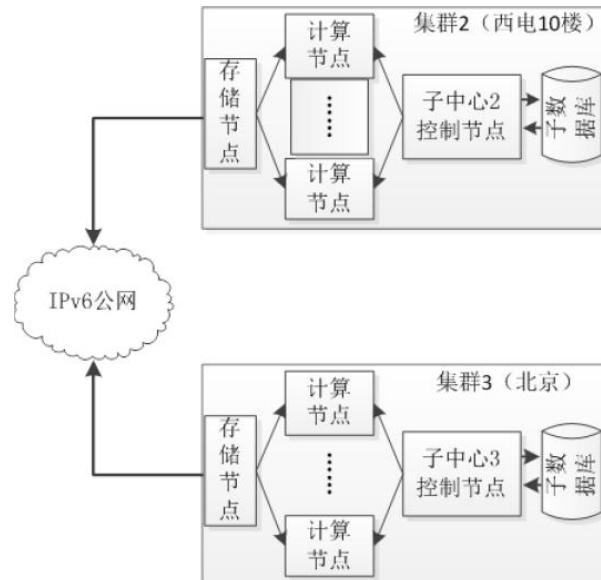
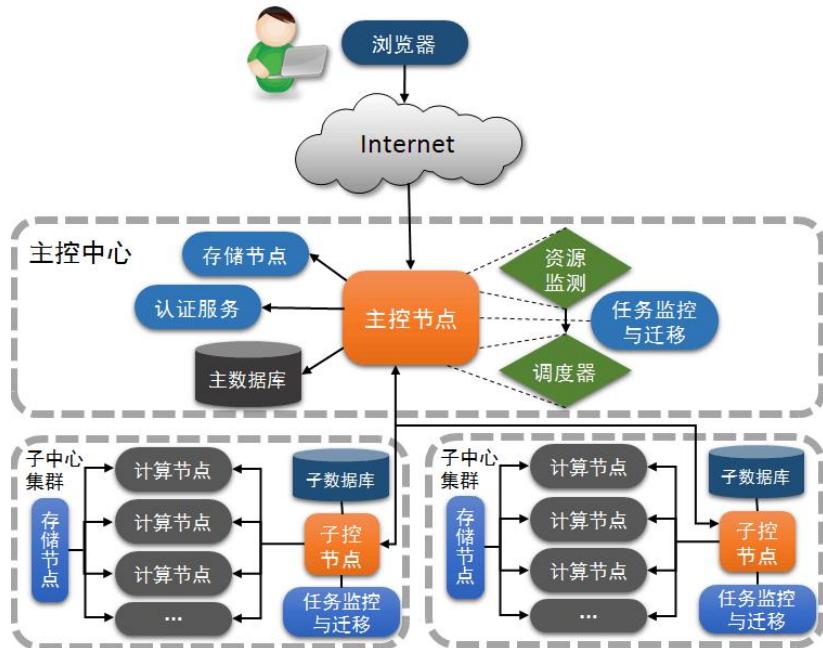
## □ 国内外技术对比

安全特性 云平台	用户接入安全	虚拟机隔离性	虚拟机监控	云平台网络安全机制	云平台后台数据库安全	云平台文件存储安全
<b>一体化安全平台</b>	用户口令+U盘+基于TPM的设备物理认证，高安全性	可信执行环境（硬件级）+虚拟化技术（软件级）	虚拟机运行时监控（宏观）+虚拟机中运行任务监控（微观）	基于可信验证的物理网络设备安全+基于虚拟防火墙的SDN安全	数据库密文存储、面向密文的数据库操作	密文对象存储、密文块存储
OpenStack	用户口令认证	虚拟机化技术（软件级隔离）	虚拟机资源消耗监控（宏观）	基于KeyStone的组件通信安全机制，无物理设备安全机制	数据库明文存储	用户文件明文存储
亚马逊AWS	用户口令认证	虚拟机化技术（软件级隔离）	虚拟机资源消耗监控（宏观）	防火墙+TLS，无物理设备安全机制	数据库明文存储	用户文件明文存储
微软Azure	用户口令认证	虚拟机化技术（软件级隔离）	虚拟机资源消耗监控（宏观）	防火墙+IDS+IPS，无物理设备安全机制	数据库明文存储	用户文件明文存储
Eucalyptus	用户口令认证	虚拟机化技术（软件级隔离）	虚拟机资源消耗监控（宏观）	防火墙+IDS+IPS，无物理设备安全机制	数据库明文存储	用户文件明文存储



## ➤ 具体应用—大规模电磁协同计算服务平台

针对大规模计算需求，设计并实现了**层次化、可伸缩安全协同计算平台**，整合分散、独立的计算资源，支持任务、资源态势的实时监控及基于资源自适应迁移的高可用策略，提供面向**电磁、气象等领域的安全的大规模计算服务**。





谢谢！

Thank You !

