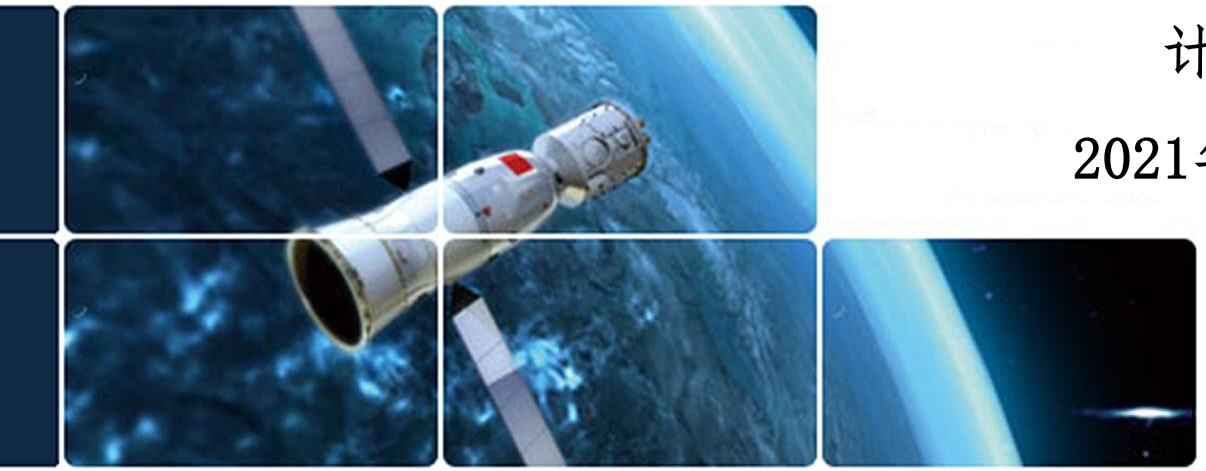
第11讲 移动互联网安全



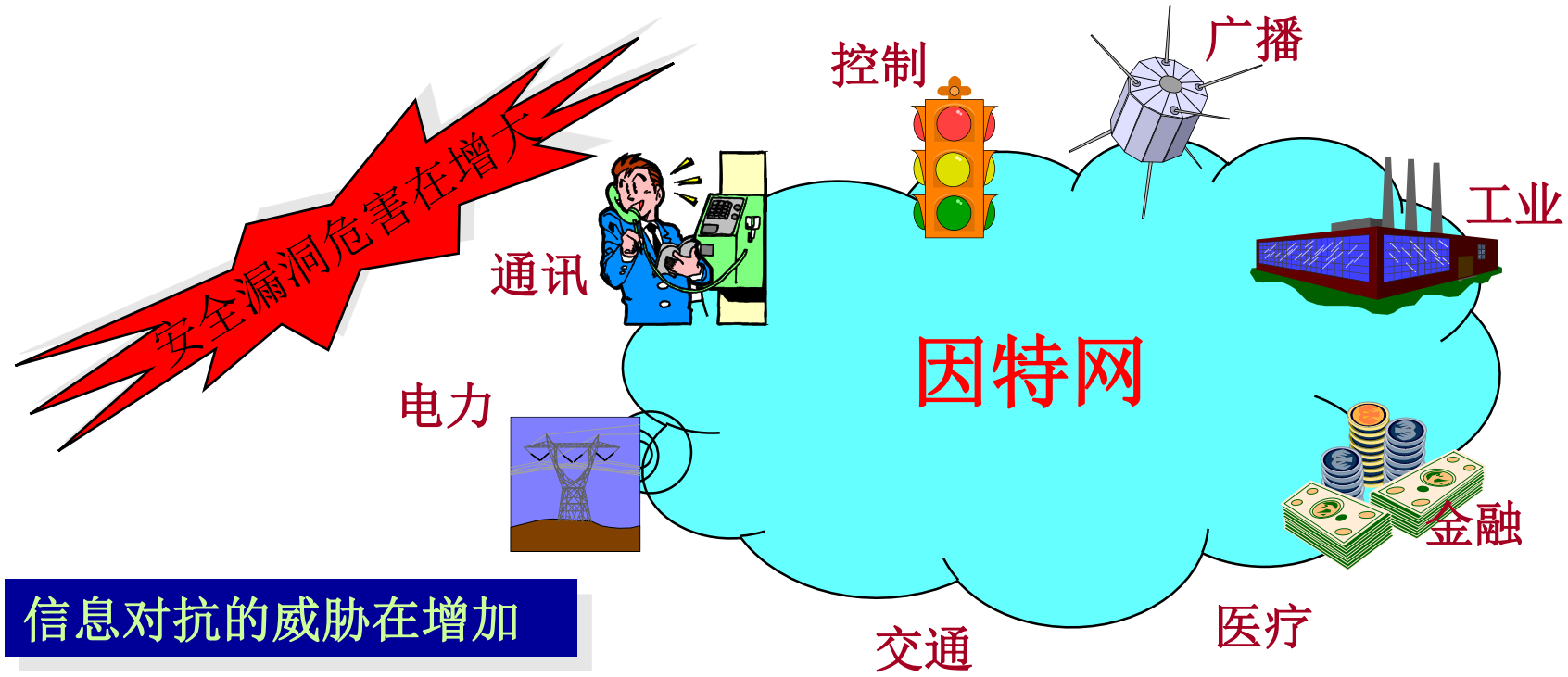
计算学部

2021年12月21日

主要内容

- **概述**
- 移动互联网安全的特点
- 移动互联网安全框架
- 移动*IP*的安全分析
- 移动*IP*的安全方案
- 数据的正确使用

网络安全威胁国家安全



信息对抗的威胁在增加

网络攻击呈现常态化、规模化和智能化趋势

网络安全的主要威胁

- 病毒，蠕虫，僵尸，木马
- 分布式拒绝服务攻击（DDOS）
- 缓冲区溢出攻击
- 网络钓鱼（欺骗手段）
- 信息泄露
- 高级可持续性攻击（APT）
- 渗透攻击（迂回式渐进式攻击）

等级保护2.0-保护对象

- 网络安全等级保护制度2.0标准于2019年12月1日开始实施

服务设施类	信息系统类	数据资源类
电信网	计算机信息系统	数据
广播电视网	工业控制系统	大数据
互联网	移动互联系统	数字资产
行业专网	物联网系统	
云计算服务平台		
大数据服务平台		
⇧	⇧	⇧
服务	信息和服务	信息

等级保护2.0-安全要求

	等级保护1.0	等级保护2.0					
		安全通用要求	云计算扩展要求	移动互联扩展要求	物联网扩展要求	工控系统扩展要求	合计
第二级	175	137	29	14	7	15	202
第三级	290	211	46	19	20	21	317
第四级	318	228	49	21	22	22	342

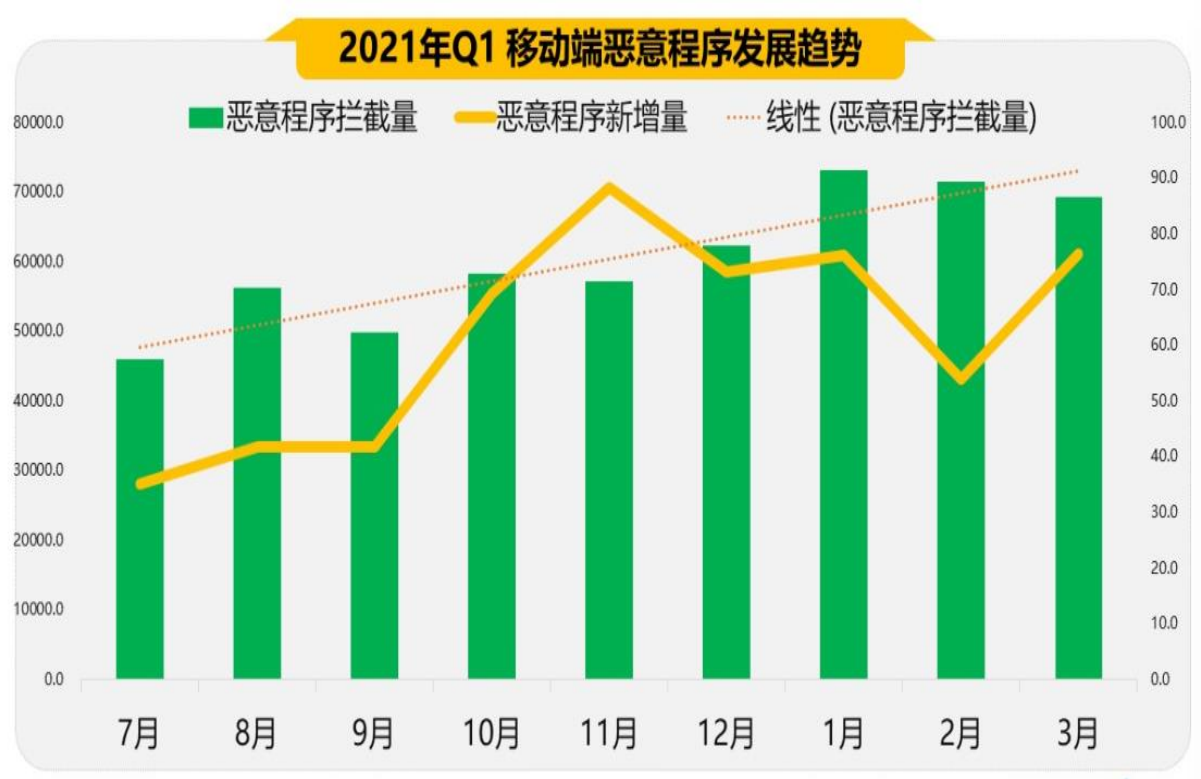
等级保护2.0-安全要求

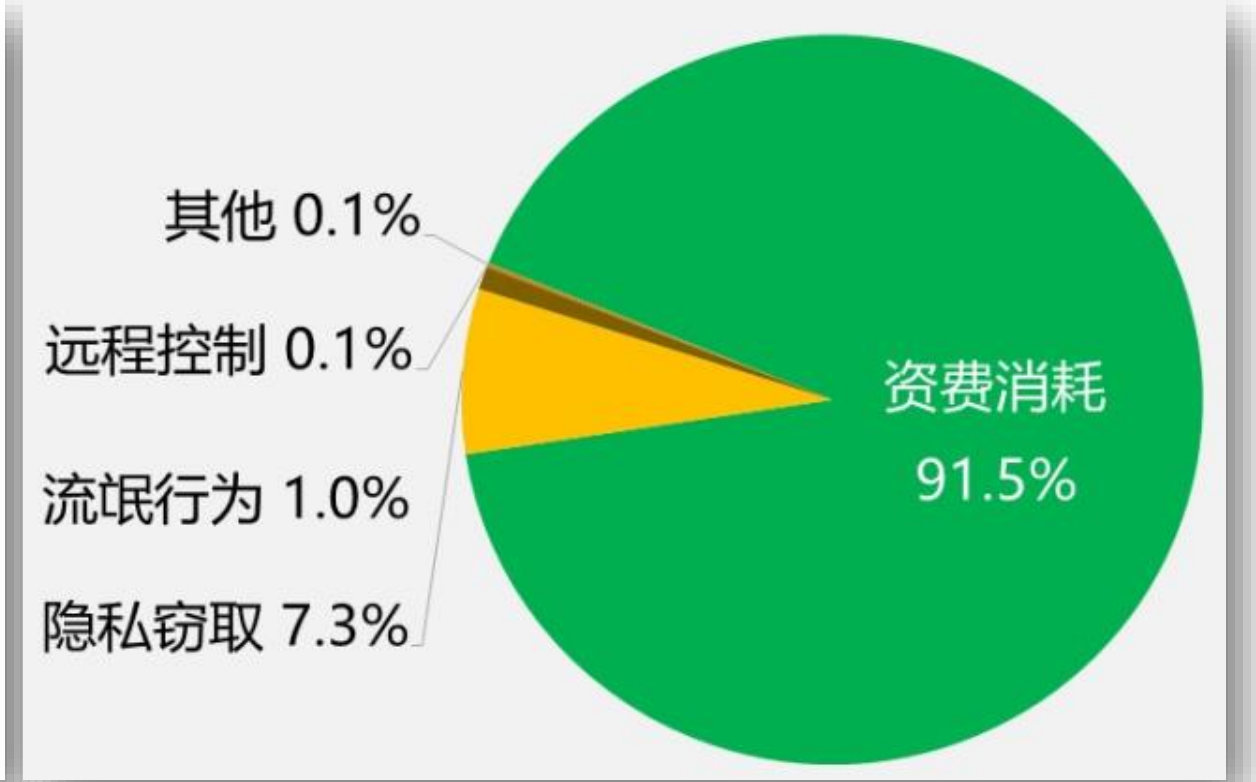
云计算安全扩展要求	移动互联安全扩展要求	工业控制系统安全扩展要求	物联网安全扩展要求
基础设施的位置 虚拟化安全保护 镜像和快照保护 云服务商选择 云计算环境管理	接入点物理位置 移动终端管控 移动应用管控 移动应用软件采购 移动应用软件开发	室外控制设备防护 网络架构安全 拨号使用控制 无线使用控制 控制设备安全	感知节点物理防护 感知节点设备安全 网关节点设备安全 感知节点管理 数据融合处理

移动互联网扩展要求

- 接入点物理位置
- 移动终端管控
- 移动应用管控
- 移动应用软件采购
- 移动应用软件开发

1. 2021年第一季度移动端恶意程序状况

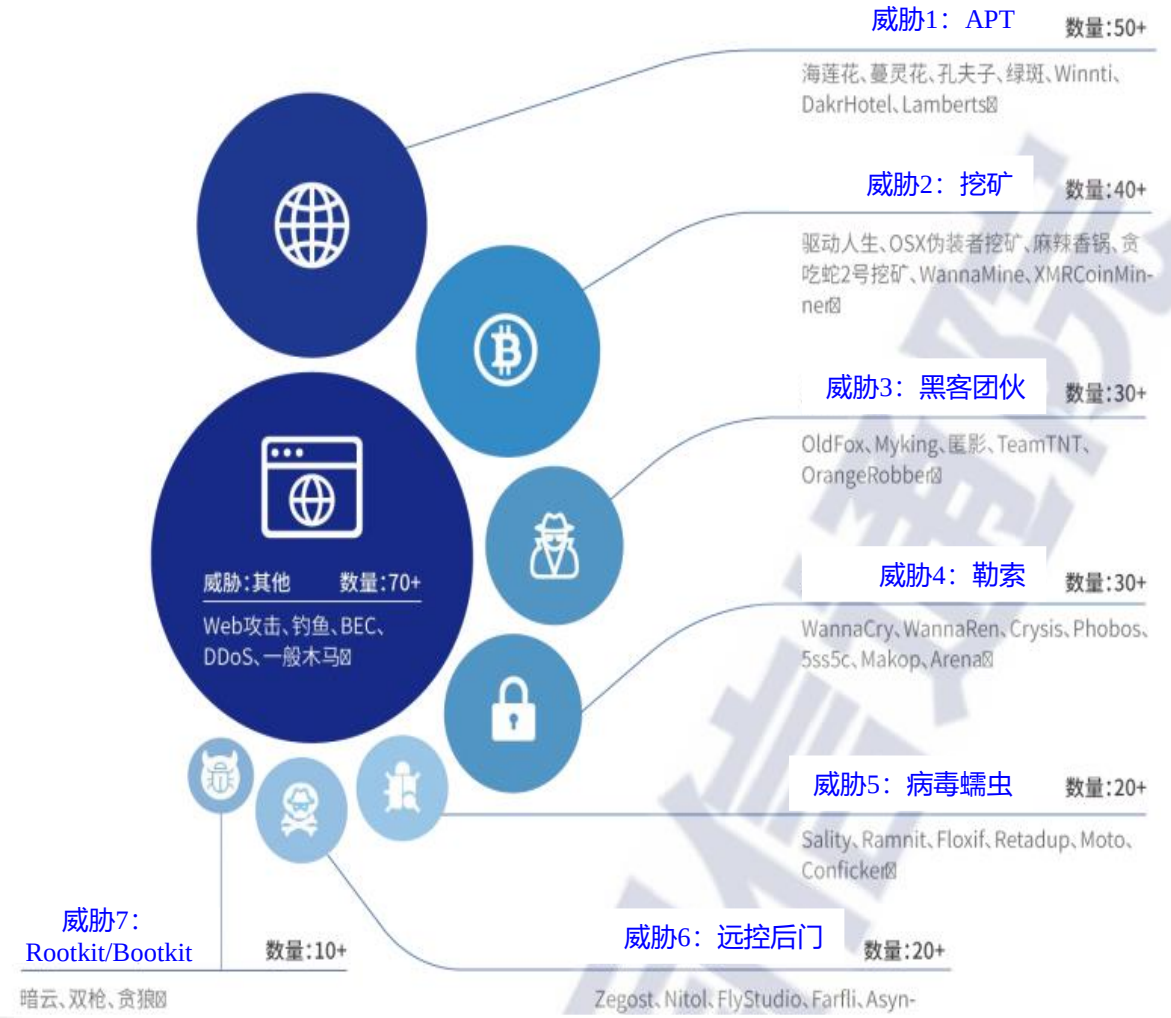




2. 2020年网络安全威胁信息

表 1 攻击者攻击活动平台分布

攻击者\OS 平台	Windows	Linux	Android	MacOS
孔夫子（Confucius）	有		有	
蔓灵花（Bitter）	有		有	
响尾蛇（SideWinder）	有		有	
肚脑虫（Donut）	有		有	
海莲花（Oceanlotus/APT32）	有		有	有
Lazarus	有	有	有	有
危险密码	有			
DarkHotel	有			
Kimsuky	有		有	
Konni	有		有	
绿斑	有			
Gamaredon	有			
APT28	有	有		
Turla	有	有		
WellMess	有	有		
APT35	有			
MuddyWater	有			
APT-C-23	有		有	
StrongPity	有			



3. 当前面临的数据安全问题

1. 数据采集环节中的安全问题	违规收集个人信息；过度索取个人权限；第三方SDK引发风险
2. 数据传输环节中的安全问题	敏感信息泄漏或篡改；中间人攻击等
3. 数据存储环节中的安全问题	明文存储个人敏感信息；移动应用数据备份缺失
4. 数据使用环节中的安全问题	数据未进行分级分类保护；敏感数据未脱敏处理；移动应用权限管理混乱；数据操作缺乏审计告警
5. 数据开放共享中的安全问题	数据开放存在数据泄漏风险；数据平台API接口安全问题
6. 数据销毁环节中的安全问题	账户注销难；数据过度留存；云端数据残留风险

移动互联网安全原因

- 基于*IP*的开放式架构是互联网安全问题的总根源
- 接入类型多样、业务丰富、上网终端智能化程度高

逐渐成为互联网安全问题的主要原因

- 互联网网络对用户透明，用户可以获得任意网络重要节点的*IP*地址并发起漏洞扫描和攻击，网络拓扑很容易被攻击者得到，攻击者可以在某一网络节点截获、修改网络中传送的数据，用户数据安全没有保障
- 用户对网络不透明，导致鉴权不严格，大量未经严格鉴权的认证机制可接入网络，终端的安全能力和安全状况网络不知情、无法控制，用户地址可以伪造，无法溯源
- 随着移动互联网时代的到来，这些问题不仅未能得到解决，相反，由于应用更加丰富，接入终端更加多样化，安全问题更加突出!

主要内容

- 概述
- **移动互联网安全的特点**
- 移动互联网安全框架
- 移动IP的安全分析
- 移动IP的安全方案
- 数据的正确使用

移动互联网安全的特点

- 移动通信与互联网融合打破了相对平衡的网络安全环境，削弱了通信网原有安全特性

（1）由于原有移动通信网相对封闭、信息传输平面和管理控制平面分离、网络行为可溯源、终端类型单一且非智能，以及用户鉴权严格，安全性相对较高，***IP***化后的移动通信网作为移动互联网的一部分，安全优势所剩无几

（2）移动互联网也是互联网的一部分，也面临互联网的安全威胁和挑战，需要提升自己的安全防护能力

（3）移动用户数量众多，参差不齐，面临的安全威胁急剧增加，带来的安全危害层出不穷，轻则影响用户的正常使用，重则影响社会的稳定、国家的安全

移动互联网的安全威胁类型

- 移动互联网环境下，业务更加丰富。应用威胁包括非法访问系统、非法访问数据、拒绝服务攻击、垃圾信息的泛滥、不良信息的传播、个人隐私和敏感信息的泄漏、内容版权盗用和不合理的使用问题
- 移动互联网环境下，终端的发展对安全提出了巨大的挑战。终端智能化、内存和芯片处理能力的增强带来了非法篡改信息、非法访问、病毒和恶意代码等新威胁；移动终端逐渐由通信工具向个人的信息处理中心转变，个人信息丢失或被窃取会造成很大损失，必须保护用户行为和隐私不受干扰
- 移动互联网所处的环境也比传统互联网更加复杂：威胁来源及脆弱性分布更广，使用者对安全防护要求更为多样化

综上，移动互联网面临三类安全威胁：业务的安全威胁、终端的安全威胁和网络的安全威胁

（1）终端安全机制：身份认证功能（口令或智能卡方式、实体鉴别方式）；安全性保护和访问控制能力（设置访问控制策略、分级存储和隔离、数据完整性检测）

（2）网络安全机制：移动网接入方面，有一套完整的安全机制，定义了更加完善的安全特征和安全服务

（3）应用安全机制：每类业务均有特定的业务标准，比如定位业务安全机制、移动支付安全机制、垃圾短消息过滤机制

移动互联网的安全任务

- 尽管*3GPP*和*OMA*（开放移动联盟）提供了各自领域的安全机制，但只是提出了可供利用的技术手段，属于基础层面，并未给出移动互联网安全的整体架构和安全部署方案，未解决移动互联网可能存在的流量攻击和不健康内容等关键技术问题
- 移动互联网安全面临的任务
  - 研究移动互联网安全总体架构，设计移动互联网中的安全能力
  - 通过安全算法、安全协议保证移动互联网基础安全
  - 研究移动互联网网络监控技术，提高对异常流量、攻击流量的防控能力
  - 研究内容过滤技术，提高对非法内容的管控力度，特别是针对使用点对点及加密方式传播的不良内容的识别、获取、分析和控制技术，并开展内容安全管理配套机制研究
  - 研究移动互联网信息安全监管系统

主要内容

- 概述
- 移动互联网安全的特点
- **移动互联网安全框架**
- 移动IP的安全分析
- 移动IP的安全方案
- 数据的正确使用

移动互联网的安全框架


安全管理
应用安全
应用访问控制
内容过滤
安全审计
网络安全
加密和认证
异常流量控制
网络隔离交换
信令和协议过滤
攻击防御与溯源
终端安全
防病毒
软件签名
主机防火墙
加密存储
密码管理
证书管理
授权管理
基础支撑

移动互联网业务来自互联网、移动网或移动网与互联网结合所得的创新业务，包括移动浏览、移动*Web2.0*、移动搜索、移动地图、移动音频、移动视频、移动广告、移动*Mashup*等业务。应用安全主要采用的安全措施包括：

（1）应用访问控制：为应用系统提供统一的基于身份令牌和数字证书的身份认证机制、基于属性证书的访问权限控制，保护受控制的信息不被非法和越权访问，并对事后的追踪提供可靠的依据。采用安全隧道技术，不经过安全隧道的访问请求一律丢弃

（2）内容过滤：包括*Web*内容过滤：选择控制、代码过滤及黑白名单/正则表达式网址过滤；反垃圾邮件：关键字匹配过滤、识别和过滤、阻断垃圾邮件源等

（3）安全审计：包括系统审计策略控制：主体鉴别、改变特权及管理安全策略的事件等；应用审计策略控制

- 移动互联网网络分为接入网及*IP*承载网/互联网，网络拓扑通常较为复杂

  - 接入网采用移动通信网时涉及基站、基站控制器、无线网络控制器、移动交换中心、媒体网关、服务通用分组无线业务支持节点（*SGSN*）、网关通用分组无线业务支持节点（*GGSN*），采用*wifi*时涉及接入设备*AP*

  - IP承载网/互联网主要涉及路由器、交换机、接入服务器等设备及相关链路

网络安全措施

- 加密和认证：可参考*WPKI*认证体系，借鉴了*PKI*主要思想
- 异常流量控制：对协议、地址、服务端口、包长等进行流量统计，基于地址特征进行会话数统计，基于策略进行流量管理和*Diffserv*服务等级设置，还可进行最大/最小/优先带宽控制和*DSCP*服务级别设置以及上下行双向流量控制
- 网络隔离交换：能实现两个互联网络的安全隔离，只允许指定的数据包在两个网络之间交换
- 攻击防御与溯源：能检测并抵抗*DDoS/DoS*攻击，基于内置事件库对攻击行为进行实时检测，在发现攻击行为后能追溯攻击源，便于事后跟踪和检查
- 指令和协议过滤：能防御针对七号信令和各种通信协议的攻击

- 防病毒。对常见的病毒和针对操作系统、应用程序漏洞的攻击具备一定的防范、防护、过滤、拦截、阻断等功能
- 软件签名。通过签名对软件进行完整性保护，防止软件被非法篡改
- 主机防火墙。在终端进行主机防火墙控制，比如黑白名单设置和数据包特征控制等
- 加密存储。包括对用户隐私信息和个人信息（通信录、通话记录、短信、*IMEI*号、*SIM*卡内信息、用户文档、图片、照片等）的保护

安全管理和基础支撑

- 安全管理：对全网安全态势进行统一监控，在统一界面下实现对所有安全设备的统一管理，实时反映全网的安全状况。能够对产生的安全态势数据进行汇聚、过滤、标准化、优先级排序和关联分析处理，提高安全事件的应急响应处置能力，还能实现各类安全设备的联防联动，有效抵挡复杂的攻击行为

- 安全基础支撑：包括秘钥管理、证书管理和授权管理

主要内容

- 概述
- 移动互联网安全的特点
- 移动互联网安全框架
- **移动*IP* 的安全分析**
- 移动*IP* 的安全方案
- 数据的正确使用

移动IP的安全威胁和攻击来源

- 移动环境
  - 移动*IP*通常应用于无线环境中，在无线网络中，攻击者可以在无线网络覆盖范围内的任意一个角落，通过无线电波发起主动攻击或者被动监听
  - 无线网络中的攻击行为比有线网络更容易实施，并且很难检测
  - 移动节点离开家乡网络，通过外地网络接入*Internet*中时，所在网不一定是可信网，也容易受到诸如窃听、重放等安全攻击
- 移动*IP*协议：移动*IP*的工作机制在一定程度上产生了新的安全隐患
  - 引入新的控制消息：代理通告、绑定更新、绑定请求/应答、代理请求/应答等，在具体实现时如果处理不当，容易引来攻击
  - 采用隧道机制：如不采取恰当的安全措施，容易受到攻击

移动IP的安全需求

- 机密性、完整性、认证和鉴权既是计算机网络的安全目标，也是移动*IP*的安全目标，其中认证和机密性更为重要
- 移动*IP*自身安全问题主要集中在：
  - （1）对注册信息的认证
  - （2）隧道中数据的安全
  - （3）移动*IP*协议实体的安全也需要保障
  - （4）不可抵赖性

移动IP的机密性需求

□对于移动*IP*而言，除了要保证通信数据的机密性外，还需要保证以下机密性：

1. 注册信息：用户注册时注册消息的机密性

2. 用户信息：用户*ID*比具体通信内容更为重要，需要采用强加密方式，以保证其机密性

3. 用户位置：移动环境中，用户使用的无线信号容易泄露用户的位置信息，移动*IP*的一些信令中也会包含用户当前所在网络的信息。用户基于隐私需要，往往希望对自己当前的所在位置保密

4. 呼叫模式：是指呼叫者*ID*、呼叫的频率、经常呼叫的通信对方等信息，偷听者一旦掌握了用户的呼叫模式，就更容易发起攻击

移动IP的认证和授权需求

- 当用户移动到外地网络时，会经常使用外地网络中的资源，通常只有授权的用户才可以访问这些资源，授权访问的前提是认证
- 认证是多样的，既有*FA*和*HA*对*MN*的认证，也有*FA*对*MN*的*HA*的认证，还可能需要*AAA*（认证、授权和记账）服务级的认证，所有认证必须是强制认证，且提供不可抵赖功能
- 在认证的基础上，确定移动用户的权限，实现授权访问，同时根据用户使用的服务进行记账

移动IP协议实体的安全需求

□移动*IP*协议实体：*MN*、*FA*、*HA*、*CN*，这些协议实体都可能受到安全攻击

（1）*MN* 。*MN*漫游到外地网络时将失去家乡网络防火墙保护，需要考虑如何将其纳入家乡网络防火墙保护中，使*MN*能够具有同家乡网络上其它固定节点相同的安全级别

（2）FA和被访问子网：当*MN*访问外地网络时，要能够在穿越外地网络防火墙的同时保护外地网络的资源和通信流

（3）家乡网络和HA： *MN*离开家乡网络后，要能够在穿越家乡网络防火墙的同时，保证家乡专用网络安全的完整性

（4）CN：要防止恶意节点假冒*MN*进行会话窃听的攻击

移动IPV4的安全分析

□移动*IPV4*工作过程主要由代理发现、注册和通过隧道传送数据几个步骤组成，从安全角度出发对几个主要步骤进行分析，可看出移动*IP*潜在安全威胁

1、移动*IP*代理发现中的安全威胁

2、移动*IP*注册中的安全威胁

3、移动*IP*隧道中的安全威胁

1.移动IP代理发现中的安全威胁

- 代理发现过程中，移动代理周期性的发送代理通告消息， *MN*根据收到的代理通告消息判断自己的位置，攻击者可以利用这种机制，伪造一个代理通告，使得*MN*遭受中间人（***Man-in-the-Middle***）攻击
- 中间人攻击是指攻击者拦截网络中的分组，经过修改之后再送回到网络中去。收到伪造代理消息通告的*MN*根据这个代理通告重新获取转交地址，从而失去和原有*FA*的联系

2.移动IP注册中的安全威胁

□当*MN*移动到外地网络，获得*CoA*之后，必须进行移动注册， *MN*向*HA*发出注册请求，*HA*返回注册应答，这样保证发往*MN*的分组能够正确路由到*MN*，攻击有以下几种：

（1）拒绝服务攻击（*Denial of Service*，*DoS*）：攻击者为阻止合法用户正常工作而采取的攻击，这是移动*IP*面临的最严重攻击类型

（2）假冒攻击：攻击者发出一个伪造的注册请求，把自己的*IP*地址当做*MN*的*CoA*时，*CN*发出的所有数据包都会被送给攻击者

（3）重放攻击（*Replay Attack*）：一种典型的假冒攻击

拒绝服务攻击

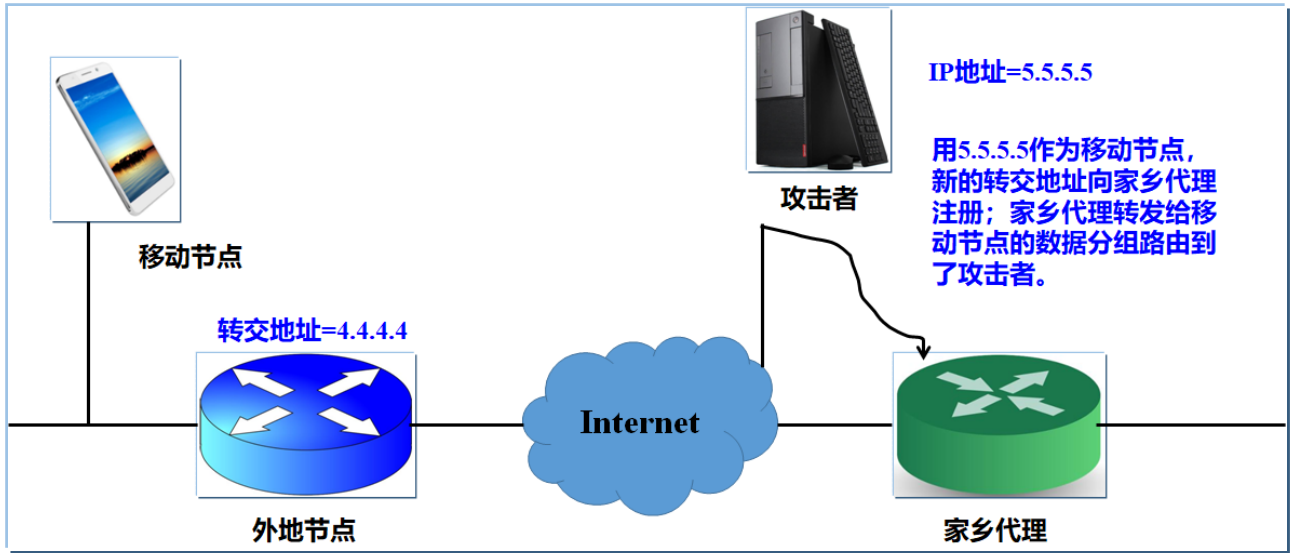
□*DoS*包括两种形式：

（1）一是通过向主机发送大量数据包，使得主机忙于处理这些无用的数据包而无法响应有用的信息；

从非法源地址建立大量的*TCP*连接“轰炸”目标主机

（2）二是对网络上两个节点之间的通信直接进行干扰，如采取重定向的方法使合法用户无法获得所需要的数据

如果攻击者注册成功，就可以截获本应送往*MN*的数据包，从而使*MN*得不到服务



拒绝服务攻击

□攻击者还可通过假冒*FA*来对*MN*发起拒绝服务攻击，当*MN*收到一条代理通告消息时，需要知道这条消息是否来自合法*FA*，如果没有认证机制，恶意*FA*很容易冒充合法*FA*

（1）向*MN*返回注册应答消息告之其注册请求消息被拒绝了

（2）将*MN*的注册请求消息传递到另外的地址，而不是传递到*MN*的*HA*上，使*MN*永远也接收不到来自*HA*的注册应答消息

（3）将*MN*的注册请求消息丢弃掉，使*MN*永远也接收不到来自*HA*的注册应答消息

假冒攻击

- 攻击者发出一个伪造注册请求，把自己的*IP*地址当做*MN*的*CoA*时，*CN*发出的所有数据包都会被送给攻击者，此时，攻击者能看到每一个送给*MN*的数据包，*MN*无法再接收到任何数据包，造成通信的中端
- 攻击者可以从无线网络覆盖的任何角落进行这种假冒攻击，攻击者只需向*MN*的*HA*发送一条伪造的注册请求消息，这可以看做是第二种形式的拒绝服务攻击

重放攻击

- 攻击者通过窃听会话，截取数据包，把有效注册请求信息保存起来，等待一段时间后，重放这个注册请求向*HA*注册一个伪造的转交地址，从而达到攻击的目的

3.移动IP隧道中的安全威胁

□利用隧道传送数据包时信息的窃取，窃取信息攻击分为网络窃听攻击和会话窃取攻击

（1）网络窃听攻击（***Passive Eavesdropping***）：攻击者偷听其它人的数据包，以窃取数据包中可能包含的机密和私有信息

移动IP使用包含无线链路在内的多种传输媒介，由于无线链路的信道特性，攻击者不需要物理链接到网络就可进行侦听，未经授权的用户也可能设法接入网络进行侦听

（2）会话窃取攻击（***Takeover***），在会话窃取攻击中，一个合法节点进行认证并开始应用会话后，攻击者通过假扮合法节点将会话窃取过去，此时合法用户无法获取有用的信息

外地链路上的会话窃取攻击

- 与偷听有相似之处。假设攻击者已通过网络链路层加密防护，位于*MN*的外地链路无线收发器覆盖范围内，或通过有线链路连接在一条基于以太网的外地链路上：

  ①攻击者等待*MN*向它的*HA*注册

  ②攻击者偷听*MN*是否开始了一个易受攻击的通信（如远程登录会话或链接到远端的电子邮箱），从中获取移动节点*CoA*等信息

  ③攻击者向*MN*发送大量无用的数据包，占用*CPU*全部时间

  ④攻击者向*CN*发送数据包，同时截获*CN*发往*MN*的数据包

- *MN*可能意识到存在问题，但并不知道被窃取。攻击者还可以窃取与*MN*在同一条链路上的主机会话，包括没有使用移动*IP*的节点及连在家乡链路上的*MN*

MN和CN路径上的会话窃取攻击

- 如果攻击者没有连到外地链路上，仍可发动会话窃取攻击，可从*MN*和*CN*之间路径上的某一点接入网络

- 假设攻击者已经攻破了网络的物理安全机制，并建立了到网络的物理连接，与外地链路上的会话窃取攻击相似。不同之处在于：

（1）在外地链路上采用的链路层加密不再有用

（2）攻击者可以窃取他所连接的链路上的所有会话，不仅仅是*MN*的会话。攻击的方法类似：先偷听，再发现目标，然后用无用数据包攻击该目标，最后假扮成被攻击节点的身份实施整个网络的攻击

移动IP隧道上的另一种安全威胁

- 如果外地网络配置了网络入境过滤的路由器或者防火墙（是指路由器或防火墙不允许源地址拓扑不正确的分组路由到网络），那么*MN*不能直接向*CN*发送数据，而需要使用反向隧道先发送到家乡网络，然后再转发给*CN*

- 利用反向隧道通信时，如果攻击者可以成功的假冒*MN*发送数据到*FA*，就能对家乡网络进行攻击，因此需要对隧道进行安全防护

在移动*IPV6*中，潜在的安全问题多数来自错误的绑定缓存，绑定缓存的产生和更改是由绑定更新和绑定确认的使用引起的，发生下述情况：

（1）*MN*向*HA*注册新的*CoA*

（2）*MN*通知*CN*它现在的*CoA*

MN向HA注册转交地址

- 攻击者伪装成***MN***，向***HA***发送非法的绑定更新***BU***，注册一个不正确的***CoA***
- 攻击者拦截***MN***发送给***HA***的绑定更新***BU***，再伪装成***HA***，给***MN***应答一个非法的绑定更新
- 攻击者拦截***MN***发送给***HA***的绑定更新***BU***，然后再重发，从而注册一个假的***CoA***
- 攻击者拦截***MN***发送给***HA***的绑定更新***BU***或者***HA***发送给***MN***的绑定确认***BA***，并作了恶意的修改

MN通知CN转交地址

- 攻击者伪装成*MN*，向*CN*发送非法的绑定更新*BU*，给出一个不正确的*CoA*
- 攻击者拦截*MN*发送给*CN*的绑定更新*BU*，再伪装成*CN*，给*MN*发送了一个非法的绑定确认*BA*
- 攻击者拦截*MN*发送给*CN*的绑定更新*BU*，然后再重发，从而注册一个假的*CoA*
- 攻击者拦截*MN*发送给*CN*的绑定更新*BU*或者*CN*发送给*MN*的绑定确认*BA*，并作了恶意的修改

移动IPV6的其它安全问题

- 目的选项扩展报头中的家乡地址选项一方面解决了网络入境过滤路由器的问题，另一方面，也暴露了*MN*当前的位置信息，这给某些希望隐藏*MN*位置信息的通信带来了安全威胁

- 目前移动*IPV6*标准规范了*IPSec*协议作为移动*IP*的安全机制。由于*IPSec*依赖于公钥基础设施（*PKI*），*IPSec*密钥管理部分要求终端设备有很强的处理能力，移动终端是计算能力相对较弱的设备，能耗也是一个需要考虑的因素，这些要求都不适合于在移动终端设备上实现

主要内容

- 概述
- 移动互联网安全的特点
- 移动互联网安全框架
- 移动IP的安全分析
- **移动IP的安全方案**
- 数据的正确使用

安全方案的设计原则

- 针对移动*IP*协议面临的多种安全威胁，安全方案须实现以下功能

（1）指令消息的完整性、认证和抗重放攻击

（2）对用户通信流的完整性、认证和机密性保护

（3）被访问网络的通信流的保密性

- 考虑到移动*IP*协议在特殊应用环境中可能遭受的安全威胁，安全方案须遵循如下原则：

（1）扩展性：*MN*在不同网络、*CN*也在不同网络，不同网络采取的安全机制可能不同，网络之间不存在必要的安全信任关系，因此需要有好的扩展性

（2）兼容性：移动*IP*协议的安全机制应该不影响所处网络的原有安全机制

（3）复杂性：安全方案尽可能简单、计算量小，还需考虑*MN*的快速切换问题

移动安全关联

□在移动*IP*的安全机制中，涉及安全关联，移动*IP*中的安全关联是一组用于保护消息的安全策略。两个移动实体进行安全通信前，必须首先协商一个安全关联，选择通信双方都能支持的加密和认证算法

□移动安全关联由以下几个部分组成：

（1）加密算法（如*DES*、*3DES*、*Blowfish*、*CAST*、*AES*等）

（2）消息摘要算法（如*MD5*、*SHA*、*Tiger*等）

（3）认证算法（如预共享密钥、数字签名和共享密钥等）

（4）移动安全关联的生存期

移动IP中的安全攻击类型

(1) 拒绝服务攻击

(2) 假冒攻击

(3) 重放攻击

(4) 网络窃听攻击

(5) 会话窃取攻击

拒绝服务攻击的解决方法

- 对付第一种拒绝服务攻击，很难甚至不可能对使用假地址的入侵者进行追踪
- 路由器通过设置入口过滤，可将源地址与其网络拓扑不匹配的数据包丢弃，可以减少*DoS*攻击的威胁，但不能完全解决，因为攻击者可以使假冒的*IP*地址正好处于网络中的某个合适节点，再继续发动攻击。入口过滤的好处是可以使追踪攻击过程更为精确，如果所有的*ISP*都设置这样的过滤器，就可能将这种攻击的数据包封锁在它的产生地
- 设置入口过滤对固定主机比较有效，但对移动*IP*来说，由于一个处于外地链路的*MN*发出的数据包的源地址仍为家乡地址，路由器认为该地址应该位于*MN*的家乡链路上，配置了入口过滤的路由器会把这些合法的数据包全部丢弃，从而造成数据丢失

拒绝服务攻击的解决方法

- ***MN***使用配置***CoA***作为发送数据包的源地址。这种方法实现简单，但存在很大的局限性，有些网络注册系统只允许***IP***地址在一定范围内的用户访问，配置***CoA***可能处于未经授权的地址范围内，从而无法享用申请的服务

- 通过使用反向隧道将数据包封装后送到***HA***，然后由***HA***负责转发收到的数据包，此时数据包的源地址与其网络拓扑相匹配而不会被入口过滤路由器丢弃。但又带来路由迂回的缺陷，而且反向隧道也要面对劫持攻击（劫持反向隧道指的是攻击者通过向***MN***的***FA***发送一个假的注册请求和注册应答来欺骗***FA***与假的***HA***地址建立隧道）

拒绝服务攻击的解决方法

◘为了对付第二种拒绝服务攻击，*MN*和*HA*之间所有的注册消息必须采用有效的认证机制，从而使得攻击者不可能伪造注册请求消息。通过认证扩展的方式提供了*MN*和移动代理之间的注册消息的认证：

（1）移动-家乡认证扩展（必选的）

（2）移动-外地认证扩展（可选）

（3）外地-家乡认证扩展（可选）

◘可根据外地的网络环境来使用可选的认证，以防止非法*MN*发起的会话窃取和*DoS*攻击，或者是假冒的*FA*发起的窃听和*DoS*攻击

◘认证的方式就是在*HA*、*MN*和*FA*之间，通过公开密钥加密和数字签名来提供相互的信任关系

假冒攻击的解决方法

- 要求*MN*和他的*HA*之间交互的所有注册消息都进行有效的认证
- 有效认证是指几乎不可能产生一个伪造的注册请求而不被家乡代理识破
- 移动*IP*采用移动-家乡认证扩展来防止假冒攻击

重放攻击的解决方法

- ***MN***为每一个连续的注册消息标识域（***Identification***）都产生一个唯一值，该值使得***HA***可以知道下一个值应该是多少，这样，攻击者就无能为力了，因为他保存的注册请求消息会被***HA***判定为已经过时

- 移动***IP***定义了两个填写标识域的方法

（1）使用时间戳，如果时间戳不相符，***HA***会拒绝注册请求，并向***MN***提供同步时钟

（2）采用***Nonces***（可选的），类似于密钥认证中随机数作用，***MN***为***HA***规定了向***MN***发送下一个注册应答消息的标识域的低半部分中必须放的值，相反，***HA***也向***MN***规定了下一注册请求消息中标识域高半部分的值，与期望值不符则拒绝

网络窃听攻击的解决方法

- 由于无线链路的物理安全性较脆弱，防止网络窃听的关键在于杜绝信息明文传输，采用数据链路层加密和端到端加密
- 数据链路层加密可以使*MN*和*FA*之间的数据在较脆弱的无线链路上传送时不被偷听；端到端加密与物理介质无关，可以在网络的任一点上保护数据
- 端到端加密可以保证数据的机密性和完整性，在通信源对数据进行加密，在目的地对数据进行解密

会话窃取攻击的解决方法

- 防止外地链路上的会话窃取攻击与防止偷听一样，至少要求***MN***和***FA***之间有链路层加密，最好是在***MN***和***CN***之间有端到端加密
- 同时提供数据加密和完整性检查是更合理的方法，解密时数据如果不能通过完整性检查，则认为是乱码，对敏感数据应同时进行加密和认证
- 对于其他会话窃取攻击，要求采用端到端加密保护网络上任意节点的数据，这种加密可以采用安全封装载荷（***ESP***）或通过应用层实现
- 加强注册过程的认证机制和对隧道的加密是理想的解决办法

移动IPV6提供的安全机制

- 移动*IPV6*标准集成了*IPSec*协议，所有*IPV6*节点均能处理认证报头（*AH*）和封装安全载荷报头（*ESP*）

- 移动*IPV6*还利用了*IPV6*的一些特性：自动配置、目的地选项和源路由。移动*IPV6*在*IPV6*的目的选项扩展报头中增加了4个新的目的选择项：绑定更新、绑定响应、绑定请求和家乡地址选项

- 在移动*IPV6*中，绑定管理是利用*IPV6*的目的地选项来实现的，所有承载了绑定更新或者绑定响应目的地选项的分组必须使用*AH*和*ESP*来认证，两种报头均可提供发送者认证、数据完整性和重放保护。另外，*ESP*报头还提供了*IPV6*分组载荷加密，解决了通信机密性所受到的安全威胁

移动IPV6提供的安全机制

- 除了使用*IPSec*，移动*IP*还采用返回路径可达过程（*RRP*）加强对通信对端绑定更新的保护

- *RRP*分为*Home RRP*和*care-of RRP*，*Home RRP*用来判断*CN*是否可以通过*HA*与*MN*的家乡地址进行通信，并且产生互相认同的*home cookie*，而*care-of RRP*用来判断*CN*是否可以直接与*MN*的*CoA*进行通信，并且产生互相认同的*care-of cookie*，两个*RRP*分别由*MN*和*CN*之间的一对消息来完成

- 家乡地址选项一方面解决了网络入境过滤路由器的问题，另一方面，也暴露了*MN*当前的位置信息，这给某些希望隐藏*MN*当前位置信息的通信带来了安全威胁。为了减少针对这种安全威胁进行的攻击，当*MN*和*CN*之间存在必要的安全关联时，家乡地址选项的功能可以和*IPSec*的*ESP*加密一起使用

不同模式下受保护的IP包

原始的数据包

传输模式受保护的IP包

隧道模式受保护的IP包

主要内容

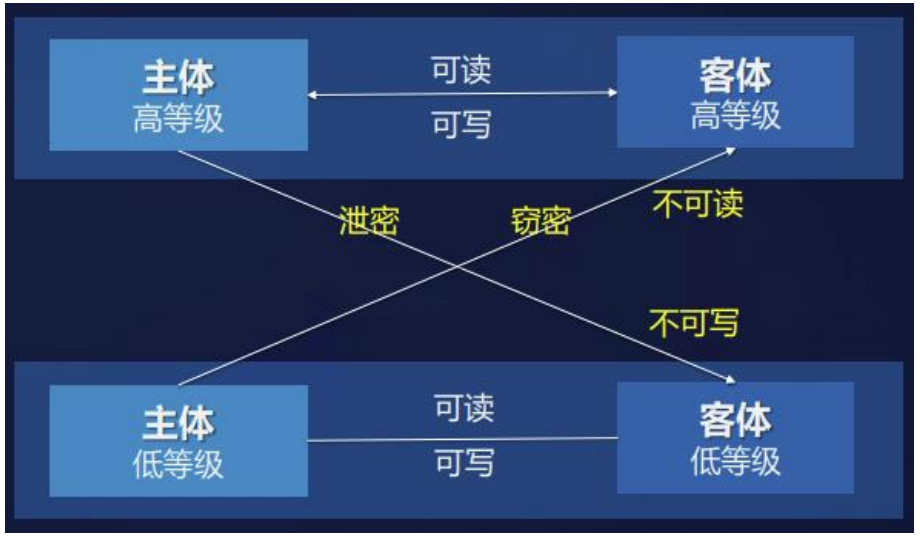
- 概述
- 移动互联网安全的特点
- 移动互联网安全框架
- 移动IP的安全分析
- 移动IP的安全方案
- **数据的正确使用**

BLP 模型核心规则

✓**不上读**-主体不可读安全级别高于它的客体（数据）

✓**不下写**-主体不可写安全级别低于它的客体（数据）

1973年，D. E. Bell 和 L. J. LaPadula 将军事领域的访问控制规则形式化为Bell&LaPadula模型，简称BLP模型。

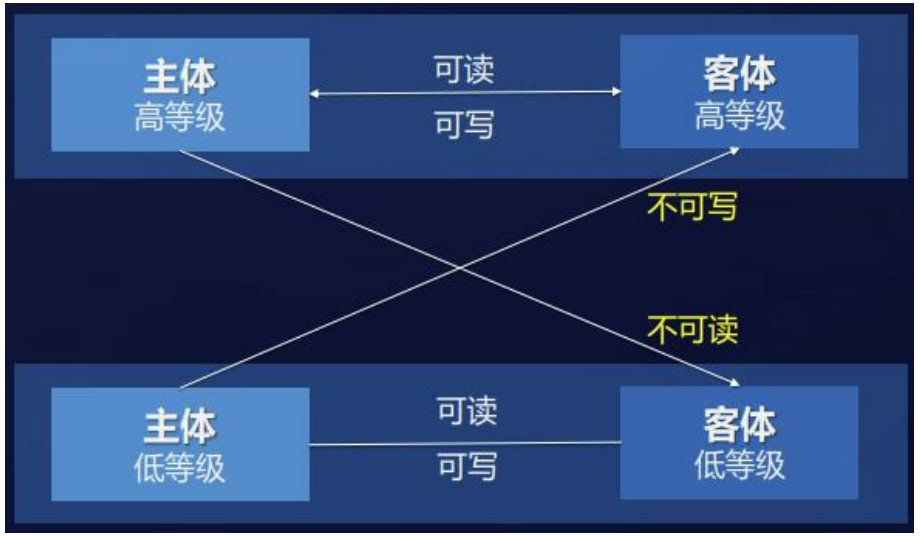


Biba模型核心规则

✓**不下读**-主体不能读取安全级别低于它的客体（数据）

✓**不上写**-主体不能写入安全级别高于它的客体（数据）

BLP模型从数学角度证明了可以保证信息隐私性，但是没有解决数据完整性的问题。就此，Ken Biba在1977年推出了Biba模型。



确保正确的人用正确的设备正确使用数据

正确
人

正确
设备

正确
使用数据

正确的人-基于零信任网络架构

用户协同认证与访问控制SDK

3 分布式跨设备互助与协同

- 持续信任等级评估
- 细粒度/持续认证与访问控制

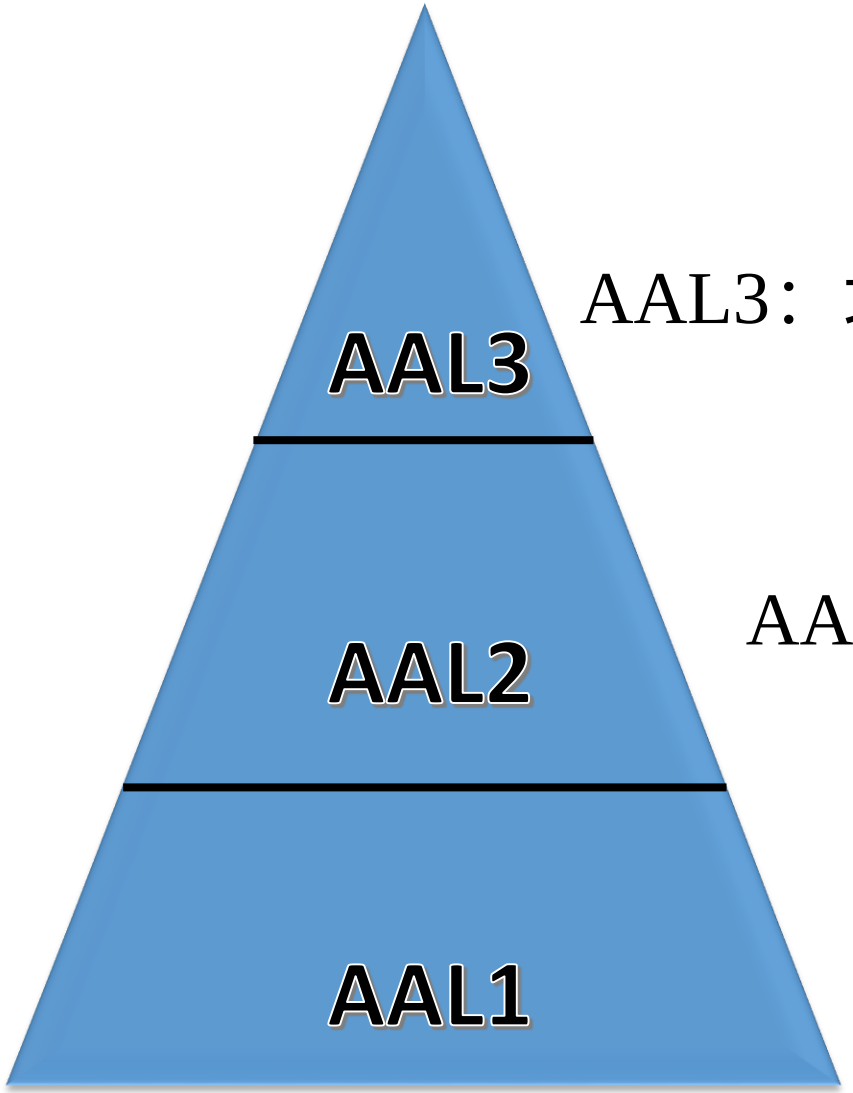
2 用户协同认证与调度

- 用户
  身份管理
- 认证器
  动态编排

1 多因素协同认证

- 秘密信息认证
  What do you know
  证明知道秘密
  - 锁屏密码
  - 应用密码
- 可信持有物认证
  What do you have
  证明持有可信物
  - 配件
  - ...
- 生物特征认证
  Who are you
  证明符合生物特征
  - 人脸
  - ...
- 持续认证
  Always be you
  证明一直是“你”特征
  - 划屏/输入
  - 声纳...

AAL分级



AAL3：增加硬件保护多因子认证

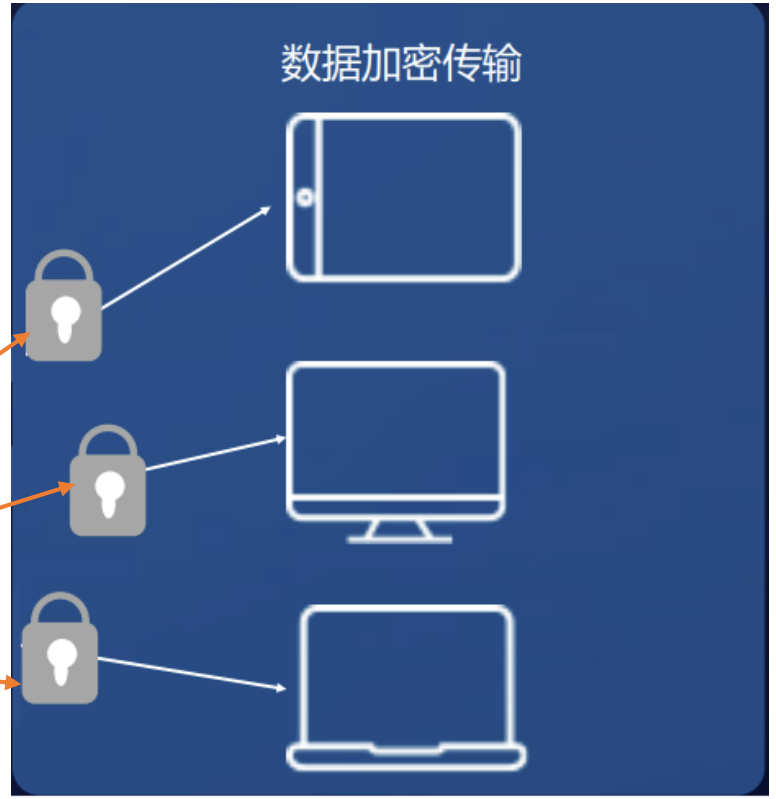
AAL2：多因子认证

AAL1：单因子认证

设备被正确的人
绑定

所连接的设备
属于正确的人

设备间传输的数据
只有正确的人可以访问



设备初始化阶段

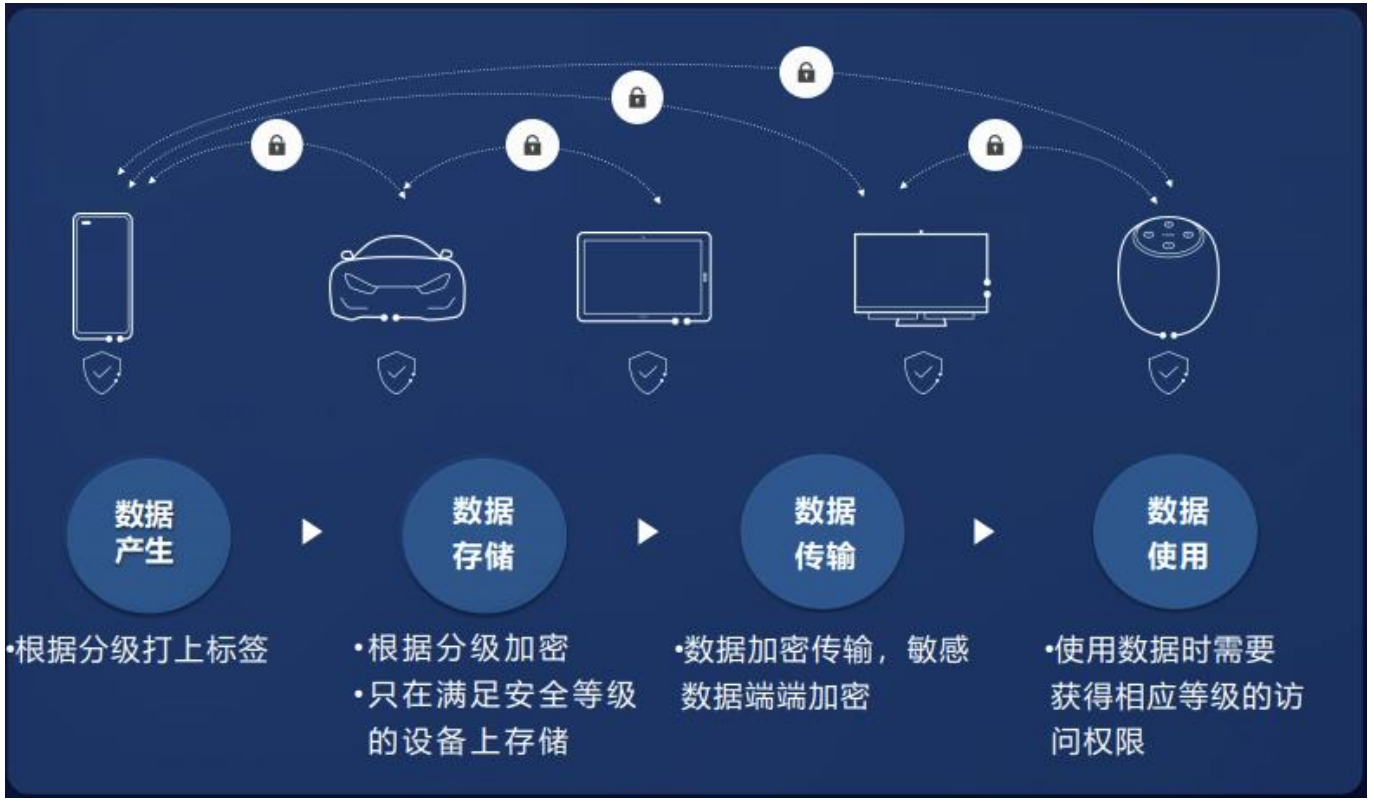
设备连接阶段

数据传输阶段

正确的设备-设备运行环境可靠安全

正确的使用数据-定义数据隐私级别

分级	举例
S4	身份认证：指纹、人脸、密码 财务数据：银行卡号、支付信息 健康信息：血压、心率
S3	运动信息：步数、距离 位置信息：GPS记录、位置历史 用户生成数据：录音、照片
S2	联系方式：电话、传真、邮箱 网络地址：IP地址、蓝牙MAC地址
S1	一般个人信息：性别、国籍、出生地 应用个性化配置：闹钟、铃声 网络状态：网络类型、网络连接状态
S0	设备型号、厂家、尺寸、版本



分布式系统设备上风险等级和加密等级的对应关系

风险等级	严重（S4）	高(S3)		中(S2)	低(S1)	公开(S0)
保护策略	锁屏下不可写	锁屏下不可写	锁屏下可写	第一次解锁前不可写	上电即可写	上电即可写

构建具有韧性的移动互联网安全系统

The End