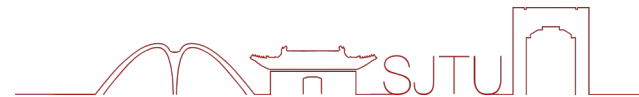




上海交通大学  
SHANGHAI JIAO TONG UNIVERSITY



# 第三章 网络安全基础

## 第二节 网络安全防护技术

主讲人：李建华 张全海  
网络空间安全技术研究院

2024 年 12 月

—— 饮水思源 · 爱国荣校 ——



1

防火墙

2

入侵检测系统

3

虚拟专网 VPN

4

计算机病毒防护技术

5

安全漏洞扫描技术



# 虚拟专网 VPN 概述

- **VPN**：（虚拟专网，Virtual Private Network）：是指将物理上分布在不同地点的网络通过公用网络连接而构成逻辑上的虚拟子网。
- **VPN 基于 Internet/Intranet 等公用开放的传输媒体**，通过**加密和认证**等安全机制建立虚拟的**数据传输通道**，以保障在公共网上传输私有数据信息不被窃取、篡改，是目前广泛应用于电子商务、电子政务等应用安全保护的安全技术。三个基本安全功能
  - ✓ **加密数据**：以保证通过公网传输的信息即使被他人截获也不会泄露。
  - ✓ **信息认证和身份认证**：保证信息的完整性、合法性，并能鉴别用户的身份。
  - ✓ **访问控制**：不同的用户有不同的访问权限。





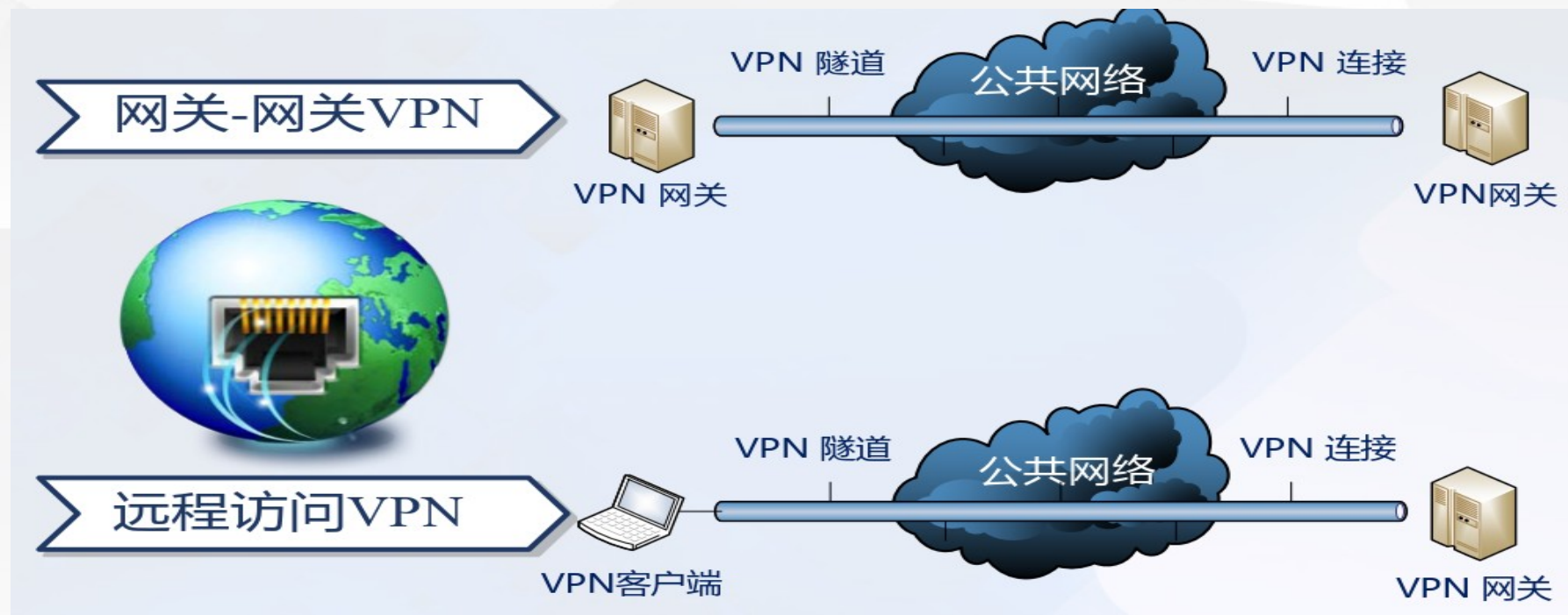
# VPN 特点







# VPN 分类



- **远程访问 ( Access VPN ) , 也称为 VPDN ( 拨号 VPN )**  
移动用户在任何地方、时间与公司总部、公司内联网的 VPN 设备建立起隧道或秘密信道，实现访问连接。
- **网关 - 网关 VPN**
  - **组建内联网 ( Intranet VPN , 企业内部虚拟专网 )**  
在公司远程分支机构的 LAN 和公司总部 LAN 之间的 VPN 。
  - **组建外联网 ( Extranet VPN , 扩展的企业内部虚拟专网 )**  
在供应商、商业合作伙伴的 LAN 和公司的 LAN 之间的 VPN 。

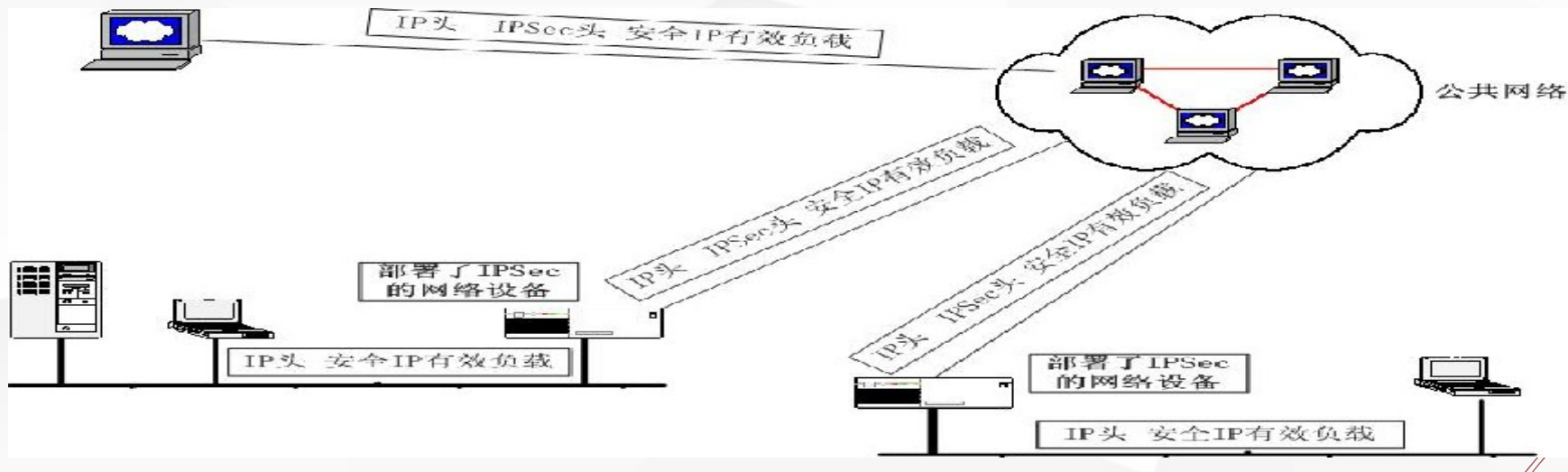






# IPSEC 协议概述

- ① IPsec 是一种由 IETF 设计的端到端的确保 IP 层通信安全的机制，为保证在 Internet 上传送数据的安全保密性能的三层隧道加密协议，弥补 IPv4 设计时缺乏安全性考虑的不足，将安全服务集成到 IP 协议中（加强 IP 协议的安全）。
- ② IPsec 是随着 IPv6 的制定而产生的，最初由 IETF 于 1995 年制定，从 1997 年开始 IETF 又开展了新一轮的 IPsec 标准修订，1998 年 11 月，主要协议已经基本制定完成。
- ③ IPsec 对 IPV4 是可选的，对 IPV6 是必须的，IPsec 由三种机制共同保障：认证、数据机密性和密钥管理
- ④ IPsec 实现两个基本目标：1 ) 保护 IP 数据包安全；2 ) 为抵御网络攻击提供防护措施。





# IPSec 体系结构

① 两大部分，三类协议构成 IPSec：两个通信协议：AH(Authentication Header，认证头)，ESP(Encapsulating Security Payload，封装安全载荷)；IKE (Internet Key Exchange)，密钥协商及交换协议

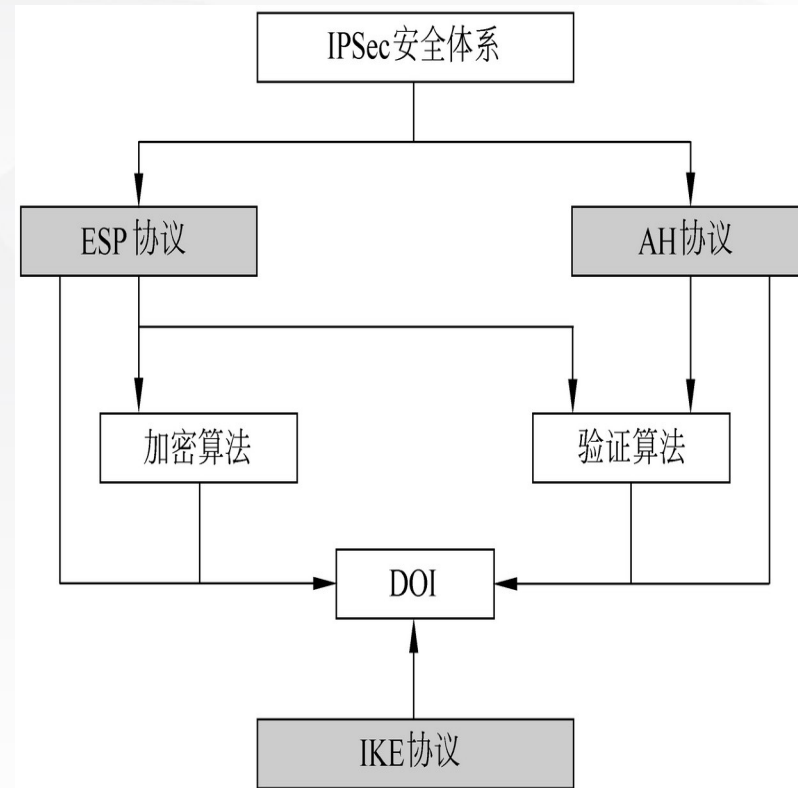
- AH 提供认证和数据完整性，ESP 具有所有 AH 的功能，还可以利用加密技术实现通信保密，这两个协议可以组合起来使用，也可以单独使用
- IKE 定义了通信实体间进行身份认证、创建安全关联 SA、协商加密算法以及生成共享会话密钥的方法

② 两种操作模式：传输模式（主机与主机的直接通信），隧道模式（常用于关联到多台主机的网络访问连入设备间使用）

③ 安全关联 SA（Security Association）：是通信对等方对某些要素的一种协定

④ 两个重要数据库：安全策略数据库 SPD，安全关联数据库 SAD

⑤ 鉴别（或验证）和加密算法



IPSec 定义了一种标准的、健壮的以及包容广泛的机制，为 IP 以及上层协议（比如 TCP 或者 UDP）提供安全保证。







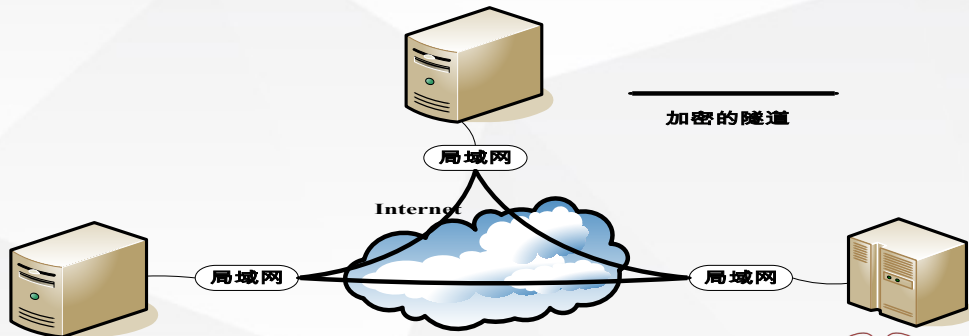
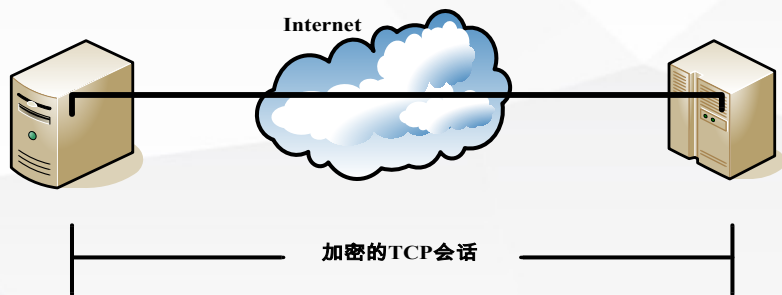
# IPSec 的工作模式

## ④ 传输模式

- 传输模式保护的是 **IP 载荷**。传输模式通常应用于**两台主机之间**，保护传输层协议头，实现端到端通信的安全性，该模式要求主机支持 IPSec。
- 当数据包从传输层传送给网络层时，AH 和 ESP 会进行拦截，在 IP 头与上层协议之间需插入一个 IPSec 头。当同时应用 AH 和 ESP 到传输模式时，应该先应用 ESP，再应用 AH。（**为什么？**）

## ④ 隧道模式

- 隧道模式保护的是整个 **IP 包**。隧道就是把一个包封装在另一个新包里面，整个源数据包作为新包的载荷部分，并在前面添加一个新的 IP 对。被封装的数据包在隧道的两个端点之间通过公共互联网络进行路由。
- **被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道**。一旦到达网络终点，数据将被解包并转发到最终目的地。
- 隧道模式应用于**网关模式**中，即在主机与网关（防火墙、路由器）或两个网关之间加载 IPSec。





# IPSec 工作模式

## 传输模式



传输模式的 AH 封装



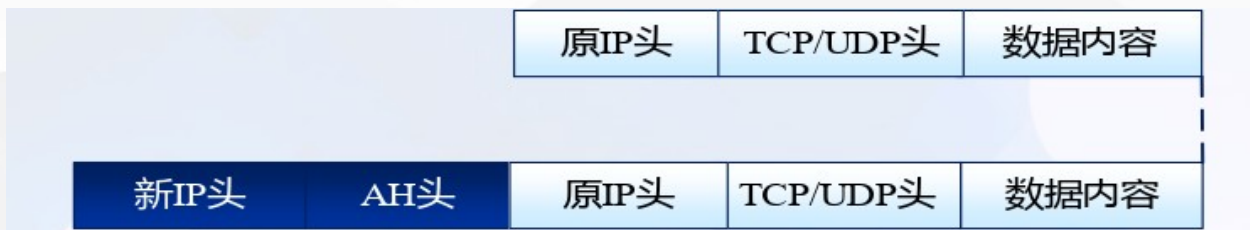
传输模式的 ESP 封装

- A. 采用传输模式时，IPSec 只对 **IP 数据包的净荷**进行加密或认证；
- B. 封装数据包继续使用原 IP 头部，只对部分域进行修改；
- C. IPSec 协议头部插入到原 IP 头部和传送层头部之间。

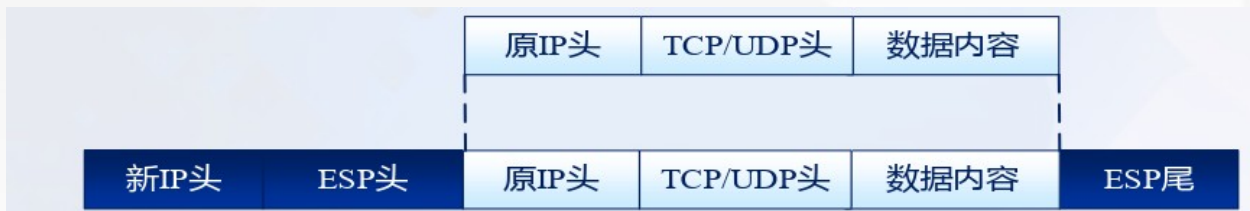


# IPSec 工作模式

## 隧道模式



隧道模式的 AH 封装







隧道模式的 ESP 封装

- A. 采用隧道模式时，IPSec 对**整个 IP 数据包**进行加密或认证；
- B. 产生一个新的 IP 头，IPSec 头被放在新 IP 头和原 IP 数据包之间，组成一新 IP 头。



# IPSec 的工作模式

	传输模式	隧道模式
AH	认证TCP、UDP或ICMP首部和数据 	认证IP首部和数据 
ESP	封装TCP、UDP或ICMP首部和数据 	封装IP首部和数据 





# TLS 协议概述

01

**SSL VPN** 也称做传输层安全协议 ( **TLS** ) **VPN** 。

**TLS**: 基于会话的**加密和认证**的 **Internet** 协议，为通信的两个实体提供了一个安全的通道。

02

**TLS** 协议主要用于 **HTTPS** 协议中，**TLS** 也可以作为构造 **VPN** 的技术。

03

**TLS VPN** 最大优点是用户不需要安装和配置客户端软件。

04

由于 **TLS** 协议允许使用**数字签名和证书**，所以它可以提供强大的认证功能。





# TLS 协议概述

选项	TLS VPN	IPSec VPN
身份验证	单向身份验证、双向身份验证、数字证书	双向身份验证、数字证书
加密	强加密，基于Web浏览器	强加密，依靠执行
全程安全性	端到端安全，从客户到资源端全程加密	网络边缘到客户端，仅对从客户到VPN网关之间通道加密
可访问性	适用于任何时间、任何地点访问	限制适用于已经定义好受控用户的访问
费用	低（无须任何附加客户端软件）	高（需要管理客户端软件）
安装	即插即用安装 无须任何附加的客户端软、硬件安装	通常需要长时间的配置 需要客户端软件或硬件
用户的易使用性	对用户非常友好，使用非常熟悉的Web浏览器，无须终端用户的培训	对没有相应技术的用户比较困难 需要培训
支持的应用	基于Web的应用、文件共享、E-mail	所有基于IP协议的服务
用户	客户、合作伙伴用户、远程用户 供应商等	更适合在企业内部使用
可伸缩性	容易配置和扩展	在服务器端容易实现自由伸缩，在客户端比较困难
穿越防火墙	可以	不可以





1

防火墙

2

入侵检测系统

3

虚拟专网 VPN

4

计算机病毒防护技术

5

安全漏洞扫描技术



# 计算机病毒防护概述

## 广义

从广义上讲，能够引起计算机故障、破坏计算机数据、影响计算机正常运行的指令或代码，均统称计算机病毒

## 规定

我国 1994 年 2 月 18 日颁布实施的《中华人民共和国计算机信息系统安全保护条例》中第二十八条规定：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码





# 计算机病毒的特征

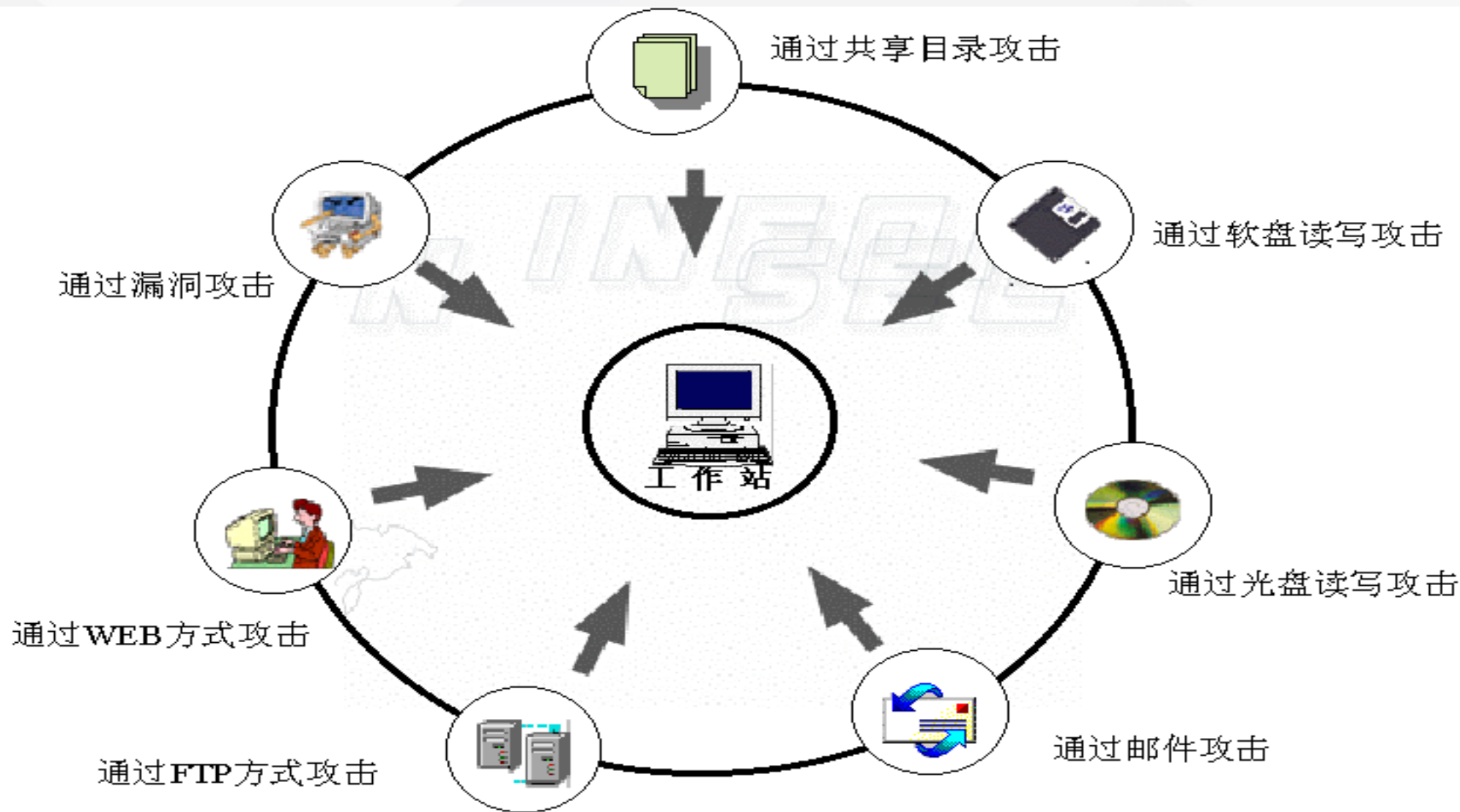


- ④ **传染性** 传染性是病毒的基本特征。计算机病毒同自然界的生物病毒一样具有传染性，会通过各种渠道扩散到更多的计算机系统上，是否具有传染性是判别一个程序是否为计算机病毒的最重要条件
- ④ **隐蔽性** 计算机病毒通常会采用隐藏进程、文件等手段延长自己的生命周期，隐藏自己的行迹，以防被发现、被删除。
  - **寄生性** 病毒通常都是附着在其它正常程序之中，类似生物界的寄生现象，当调用程序时窃取到系统的控制权，先于正常程序执行。 **现在这个特性正在变化**
  - **潜伏性** 大部分的病毒感染系统之后不会马上发作，可长期隐藏在系统中，只有在满足其特定条件时才启动其表现（破坏）模块
- ④ **破坏性** 任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响，如降低计算机工作效率，占用系统资源，导致系统崩溃





# 计算机病毒传播方式





# 计算机反病毒技术与发展历史

反病毒的核心思想：在病毒的存储、传播和执行等阶段，  
基于“发现”“拦截”“清除”等基本手段来对抗病毒  
反病毒技术和形式从发展初期至今经历了三个主要阶段：

## 第一阶段

基于**简单特征码**查杀的  
单一专杀工  
具阶段

## 第二阶段

基于**广谱特征码**查杀、  
主动防御拦  
截的综合杀  
毒软件阶段

## 第三阶段

基于**云、人工智能和大  
数据**技术的  
互联网查杀  
阶段。



# 计算机病毒分类



木马型  
病毒

感染型  
病毒



蠕虫型  
病毒



后门型  
病毒



恶意软  
件







# 计算机病毒主流检测技术

## 病毒检测原理

采样

匹配

基准

### ● 基于特征码的传统检测技术

采样为固定位置、采用精准匹配方式  
技术简单、易于实现、查杀精准  
速度慢、无法查杀未知病毒

### ● 基于行为的传统检测技术

针对病毒动态行为进行检测  
针对隐蔽性强的病毒有更好检测  
能力，具备查杀未知病毒能力

### ● 基于云技术的云查杀技术

将“匹配”和“基准”放在云端进行  
反应速度快  
终端资源使用大大减小

### ● 基于大数据与人工智能的查杀技术

将“匹配”和“基准”放在云端进行  
可以根据模型匹配已知与未知病毒





1

防火墙

2

入侵检测系统

3

虚拟专网 VPN

4

计算机病毒防护技术

5

安全漏洞扫描技术



# 漏洞概述

**漏洞** ( Vulnerability ) 又叫脆弱性，是信息技术、信息产品、信息系统在设计、实现、配置、运行等过程中，**有意或无意产生的缺陷**，这些缺陷以不同形式存在于信息系统的各个层次和环节之中，而且随着信息系统的变化而改变。**一旦被恶意主体所利用，就会造成对信息系统的安全损害**，从而影响构建于信息系统之上正常服务的运行，危害信息系统及信息的安全属性。

针对不同的对象描述漏洞的概念，综合分析可以发现漏洞有以下几个特点：

- 漏洞是信息系统**自身的弱点和缺陷**；
- 漏洞**存在于一定的环境中**，寄生在一定的客体上；
- 具有**可利用性和违规性**；本身的存在虽不会造成破坏，但是可以被**攻击者利用**，从而给信息系统安全带来威胁和损失





# 漏洞扫描技术概述

**漏洞扫描**即针对通用**漏洞**的检测，需要依据通用漏洞的形成原理和其造成的外部表现来判断。由系统维护人员识别**安全风险**，依据结果对漏洞实施有针对性的防护或修补。

漏洞按照被公布时间的不同阶段，可分为：

1 Day 漏洞

发现并公布的  
最新漏洞

N Day 漏洞

被公布的历史漏  
洞

0 Day 漏洞

未被公开的漏  
洞

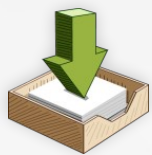




# 漏洞扫描技术概述

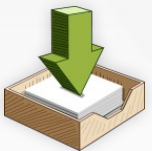
随着计算机系统普及和网络基础设施的建设，各类漏洞规模急剧扩充，为了有效量化管理，国际上不同组织提出了**各类漏洞管理标准**：

国外



**MITRE CVE**、**CWE**、**NIST NVD**、**Symantec BUGTRAQ** 等

国内



中国信息安全测评中心维护的 **CNNVD** 国家信息安全漏洞库，国家互联网应急中心 **CNCERT** 维护的 **CNCVE**、**CNVD** 国家信息安全漏洞共享平台等

依赖  
因素

漏洞  
Poc ( Proof  
of Concept )  
是否公开：  
Poc 是通用漏  
洞存在的原理  
证明

系统指纹信息采集准  
确度：原则上识别出  
目标系统，就可判断  
相应漏洞是否存在

漏洞  
EXP ( EXPloit ) 是否  
存在：EXP 为按照通  
用漏洞缺陷原理，针对  
相应实例加以利用

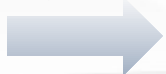




# 漏洞扫描技术分类



系统扫描



扫描目标是已规模化发布的系统、应用软件或者设备。

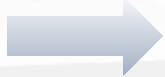
操作系统	网络设备	协议 / 端口	服务应用
Windows 系列	Cisco 设备	ftp/21	Apache
Mac 系列	华为设备	http/80	Tomcat
Linux 系列	3com 设备	Telet/23	Nginx
其他	TP-LINK 设备	smtp/25	MySQL
	其他设备	其他协议	其他应用



# 漏洞扫描技术分类



应用扫描



扫描目标是各种应用，以 Web 应用居多。

## 内容管理系统

用友

通达 OA

大汉

拓尔思

其他

## 服务器

Apache

IIS

Tomcat

Weblogic

其他

## 框架

Struts2

Spring

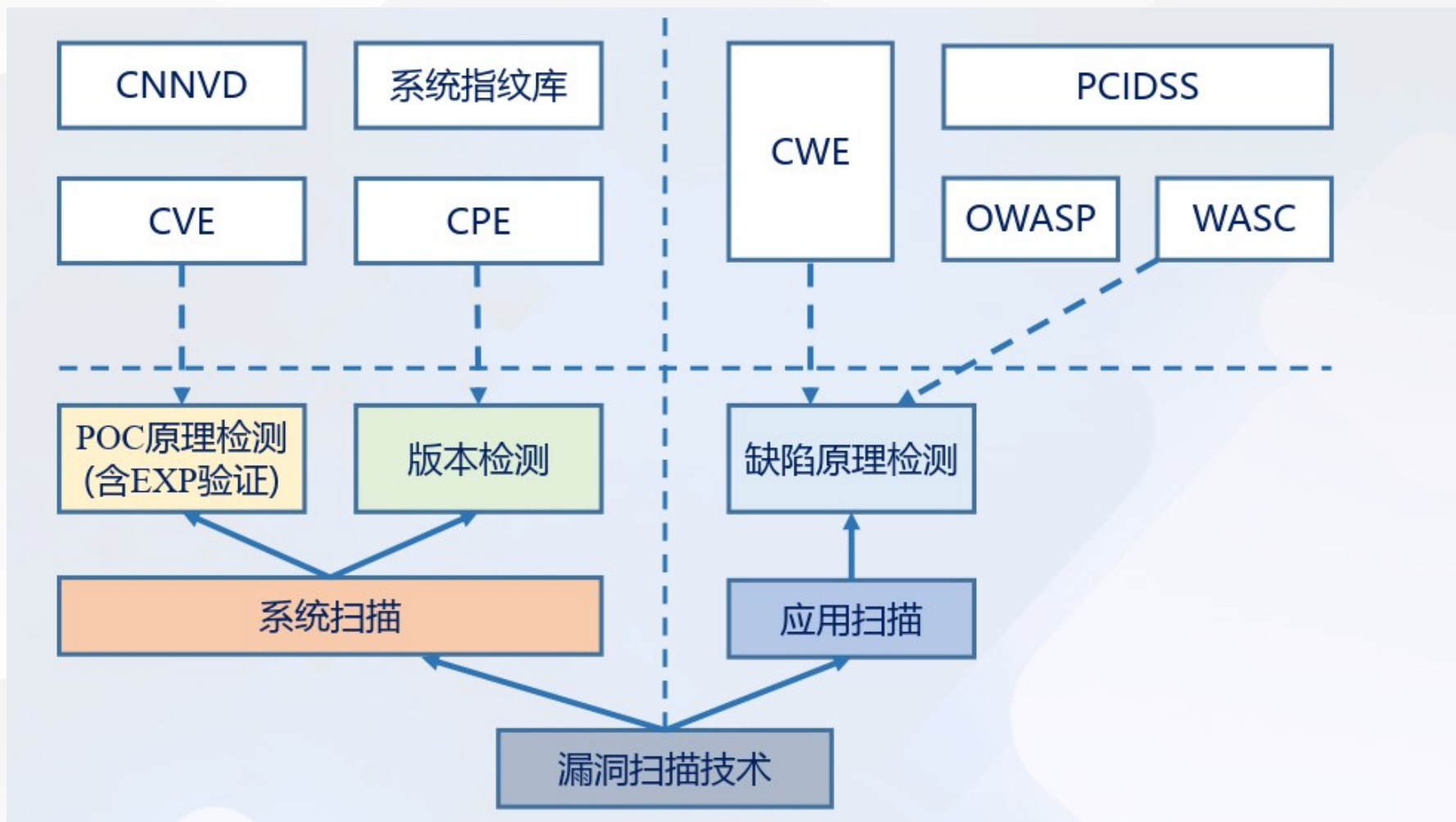
jQuery

其他



# 漏洞扫描技术分类

按照漏洞扫描的目标对象类型维度划分

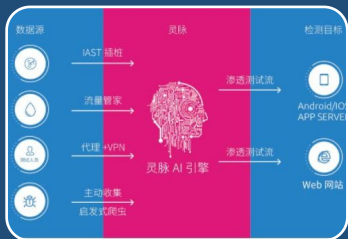


# 漏洞扫描技术分类



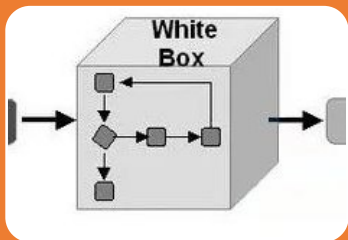
## 黑盒扫描（动态应用程序安全测试）DAST

- 将扫描对象看成黑盒，不改变和深入内部
- 从外部识别漏洞或缺陷



## 交互式扫描（交互式应用程序安全测试）IAST

- 目标内部植入扫描代理，与外部扫描设备互动
- 扫描代理进行内部监控，并对外反馈



## 白盒扫描（静态应用程序安全测试）SAST

- 代码（源代码、二进制文件）审计
- 扫描漏洞、代码质量评估、编码规范符合度审查等





# 漏洞扫描原理简介

## 存活判断

为保证扫描效率，启动扫描任务前  
会首先探测目标系统是否存活



## 端口扫描

对已经存活的主机，需要探测主机  
上开启了哪些端口



## 系统和服务识别

采用黑盒测试方法，通过研究其对  
各种探测的响应形成识别指纹，进  
而识别目标主机运行的操作系统



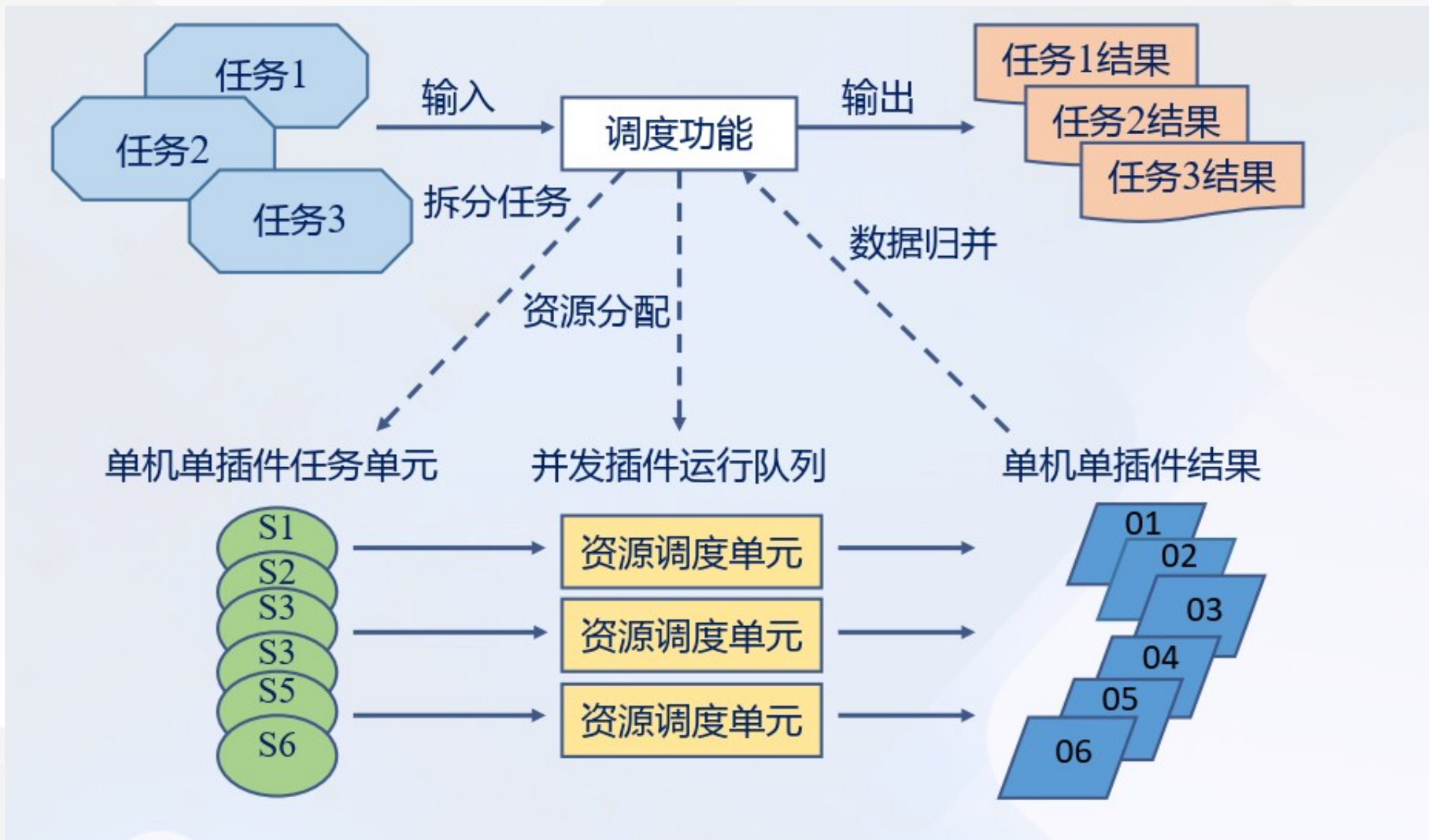
## 漏洞检测

扫描器根据识别的系统与服务信息调用内  
置或用户外挂的口令字典进行口令猜测，  
并同时启动远程非登陆漏洞扫描





# 漏洞扫描原理简介





# 漏洞扫描原理简介

## 原理检测 (POC 检测)

对目标机的相关端口发送请求构造的特殊数据包，进而根据返回的结果信息，判断漏洞是否存在。

## 版本检测

系统扫描是依照漏洞库标准实施的，在标准的漏洞说明中，会详细说明该漏洞所在系统的身份信息，例如 CPE 标识的系统类型和详细版本号。此外按照惯例，系统的升级一般会更改版本号，因此在漏洞与系统版本之间就存在了关联关系。



上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

谢谢！



饮水思源 爱国荣校