

# 《计算机文化基础》课程

# 计算机网络与网络安全

Overview of computer networks & cyberspace security

陆超逸

清华大学 网络科学与网络空间研究院 博士后

2024年12月

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 第一部分 Part I

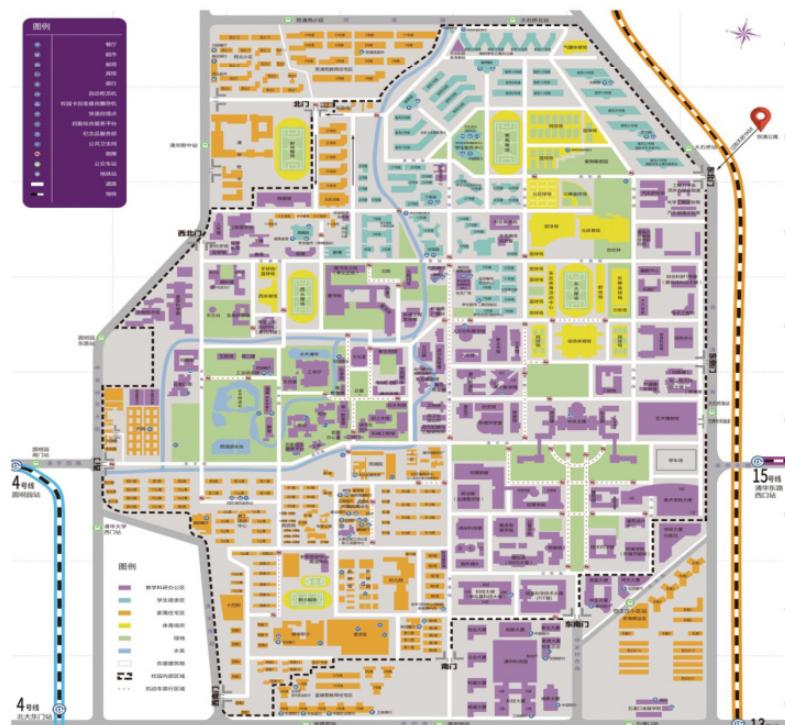
## 计算机网络引论

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

这是一个关于信息传递的故事。

## 故事要从 一位饿了的同学开始——

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用





5



6



7



8



9



10

## 版本0.1 引入代理人的 “人肉”实体信息传递

发送方、接收方引入  
信息传递的代理人  
以节省资源

“我想点【一份海南鸡饭加一杯酸梅汤】  
【多加酱油不要香菜】，请送到【教学楼】”

点餐前台

目标餐厅



当前所在地  
(教学楼)



暖心室友

暖心室友

暖心室友



11

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 版本1.0 “虚拟”信息传递

通过传播速度更快的  
电信号传递信息

“我想点【一份海南鸡饭加一杯酸梅汤】  
【多加酱油不要香菜】，请送到【教学楼】”

目标餐厅

代理设备  
(电话)

当前所在地  
(教学楼)



代理设备  
(电话)

端 (peer)

通信双方使用的对等代理设备



12

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 版本1.1 加入“暗号”的 “虚拟”信息传递

通信双方存在  
事先协商好的约定  
便于理解、提升效率

思考：  
根据你的生活经验，依靠电话  
传递信息，存在哪些不足？



13

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 版本2.0 借助计算机的 “点对点”信息传递

借助计算机进行通信  
进一步提升效率

“【A套餐一份】，  
【1号需求】， 【甲地】”

客户端 Client  
(计算机)

服务器 Server  
(计算机)

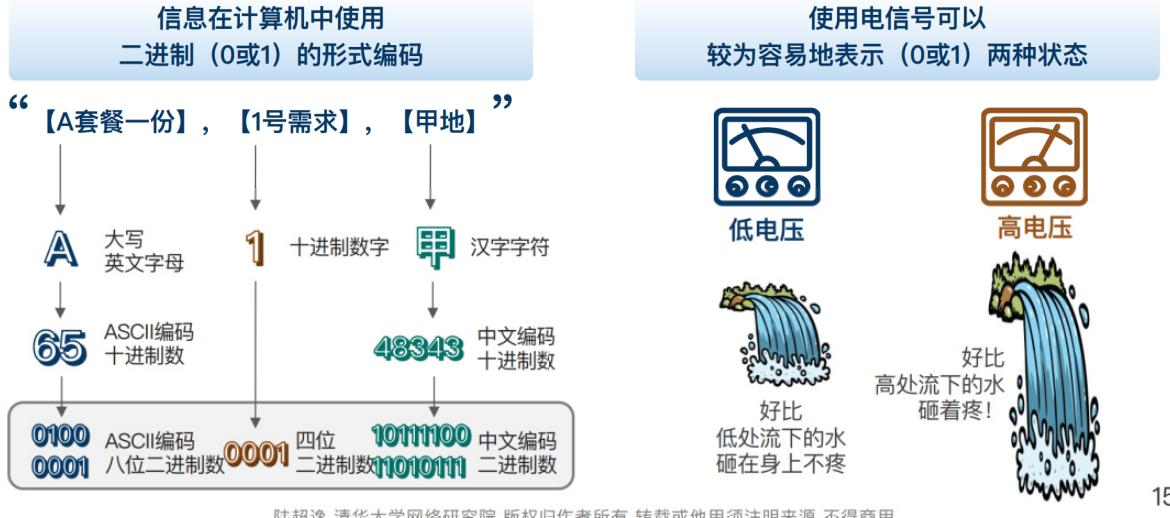


14

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

# 计算机之间的通信介质：电缆与电信号

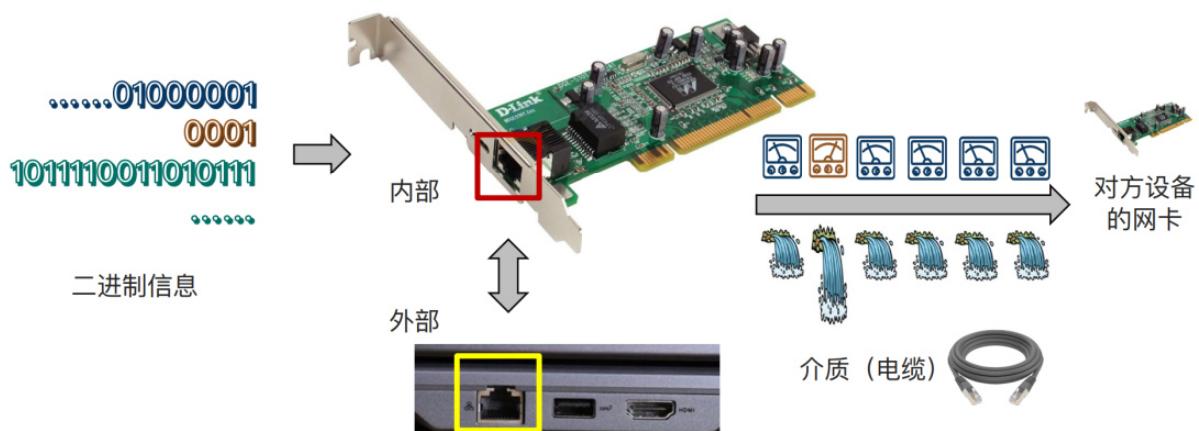
为什么两台计算机通过电缆连接起来，理论上就具备了通信条件？



15

## 二进制信息和物理信号的转换

由计算机中的网络适配器（network adaptor, 俗称网卡）实现



16

**版本2.0**  
借助计算机的  
“点对点”信息传递

借助计算机进行通信  
进一步提升效率

信息传递用时: <1秒



目标餐厅

服务器 Server  
(计算机)

**客户端-服务器 (C/S) 模型**

将网络应用（点外卖）分为两部分  
客户端：发出请求（点餐）的一端  
服务器：提供服务（出餐）的一端

电缆



当前所在地  
(教学楼)



思考：

版本2.0在后续发展的过程中，可能  
会遇到什么问题？

.....01000001  
0001  
10111001101011.....

“【A套餐一份】，  
【1号需求】，【甲地】”

客户端 Client  
(计算机)

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

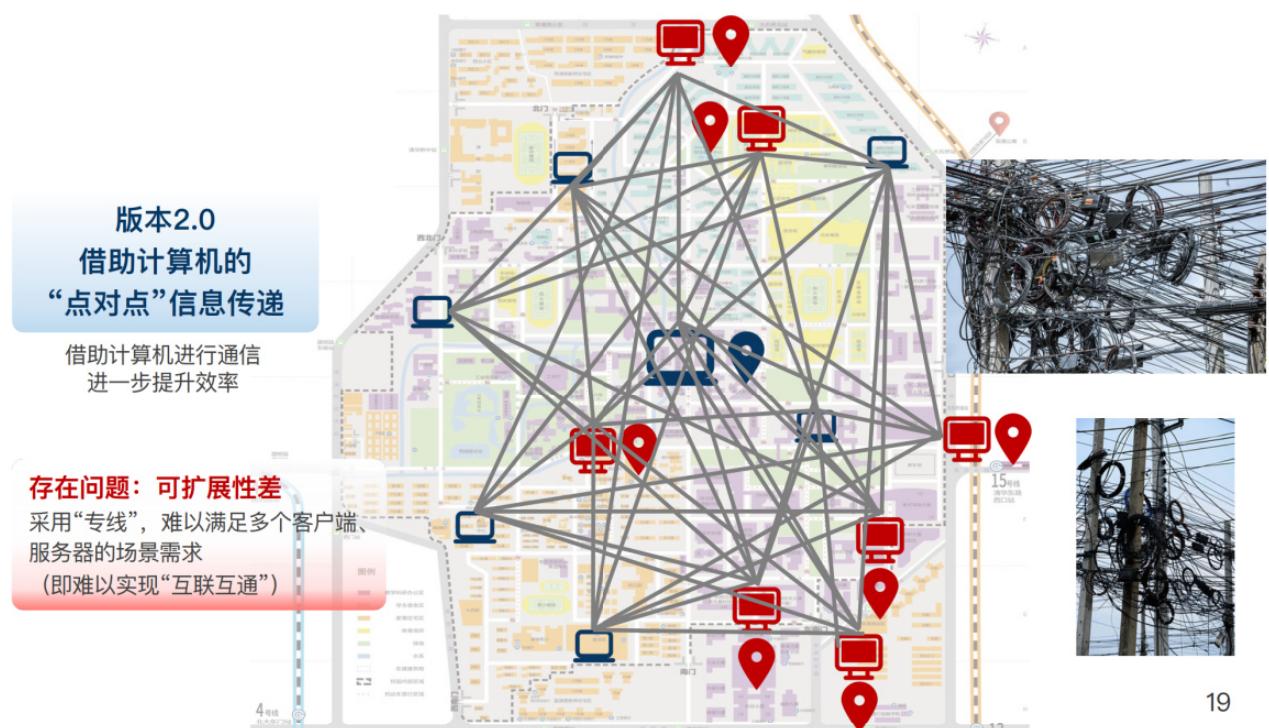
17

**版本2.0**  
借助计算机的  
“点对点”信息传递

借助计算机进行通信  
进一步提升效率

4号线  
北大东门站

18

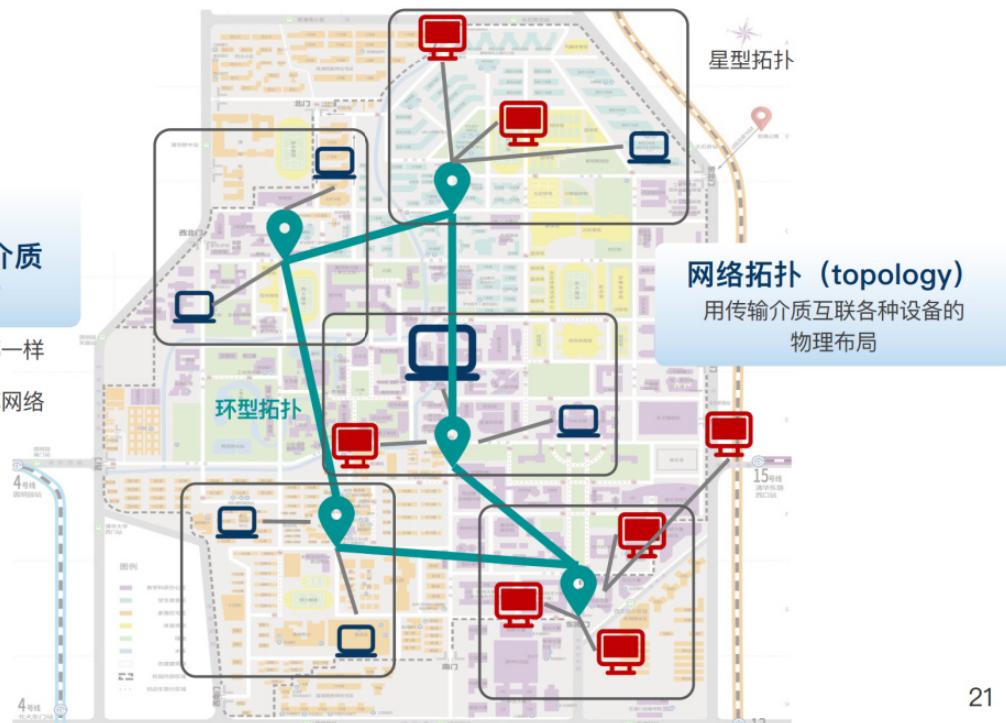


**版本3.0**  
**共用信息传输介质**  
**“分而治之”**

你的电缆我的电缆都一样  
构建有组织的  
计算机间的信息共享网络

星型拓扑

**网络拓扑 (topology)**  
用传输介质互联各种设备的  
物理布局



21

## 计算机网络的组织：网络交换设备

哪些设备在充当“路口”的作用？

终端设备



计算机

房间里的



家用路由器

楼栋里的



交换机房

地区内的



大型网络机房

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

22

# 计算机网络的组织：网络运营商

“路口”以及它们之间的线路，由谁来搭建和维护？

国内的“三大运营商”



中国教育和科研计算机网 (CERNET)

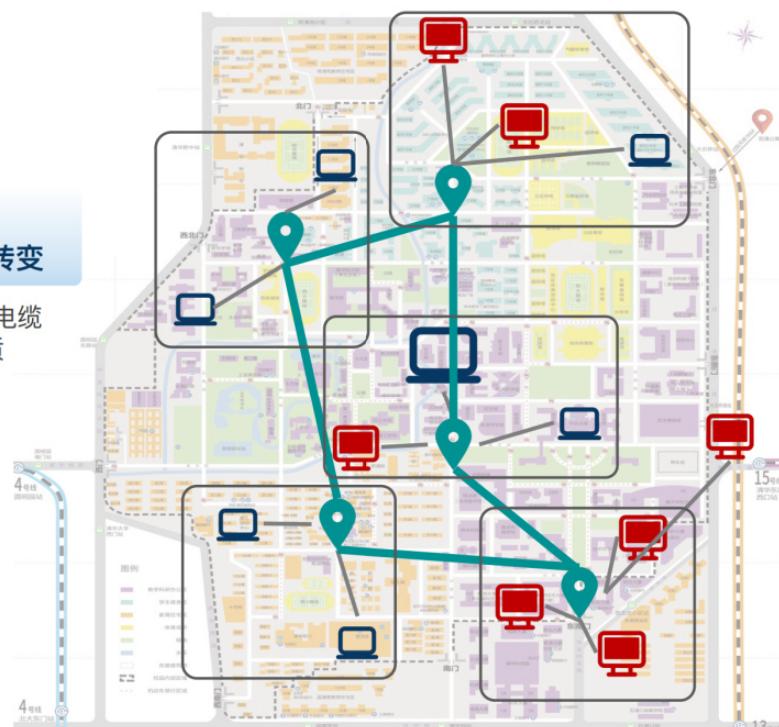


23

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

版本3.1  
有线向无线的转变

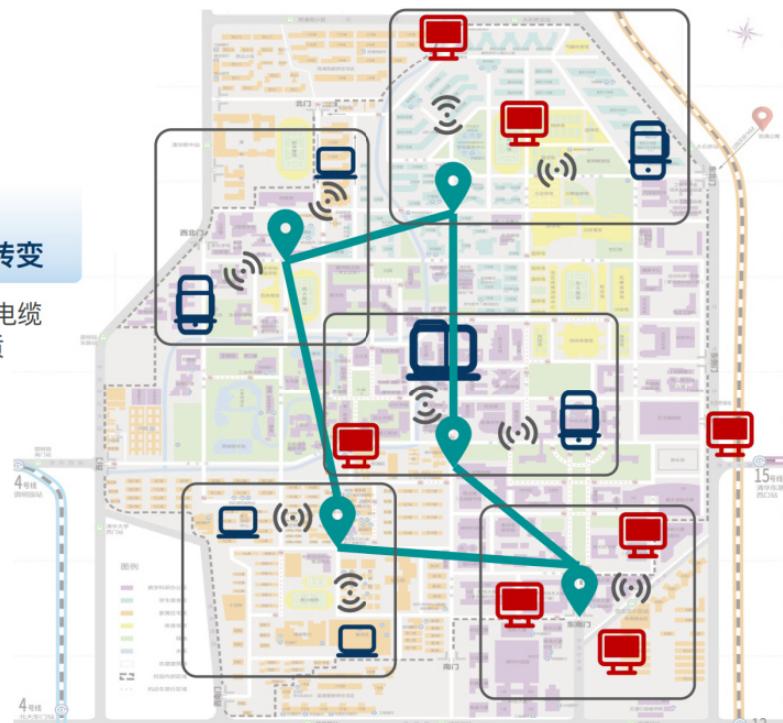
使用电磁波代替电缆  
作为传输介质



24

**版本3.1  
有线向无线的转变**

使用电磁波代替电缆  
作为传输介质

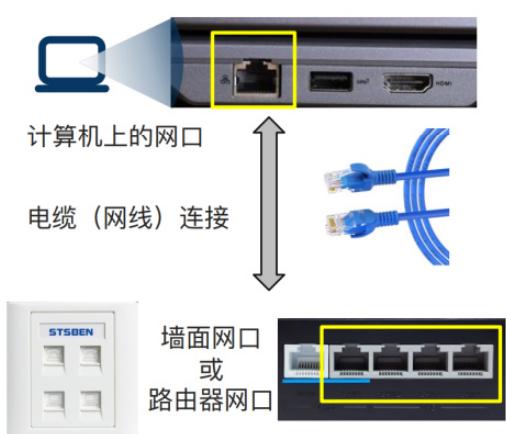


25

## 传输介质的变化：从有线到无线

电磁波代替电缆连接，使得终端设备更加方便地接入网络

**通过有线介质（网线）接入**

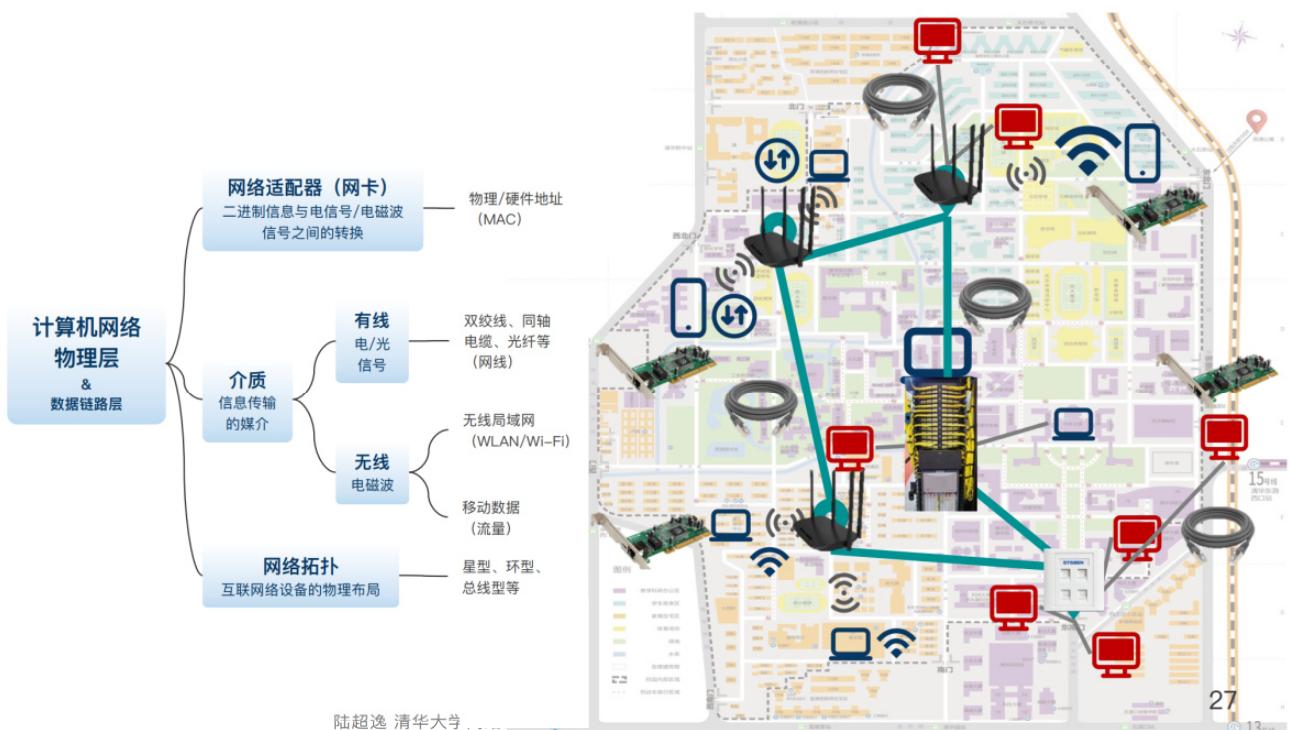


**通过无线介质（电磁波）接入**

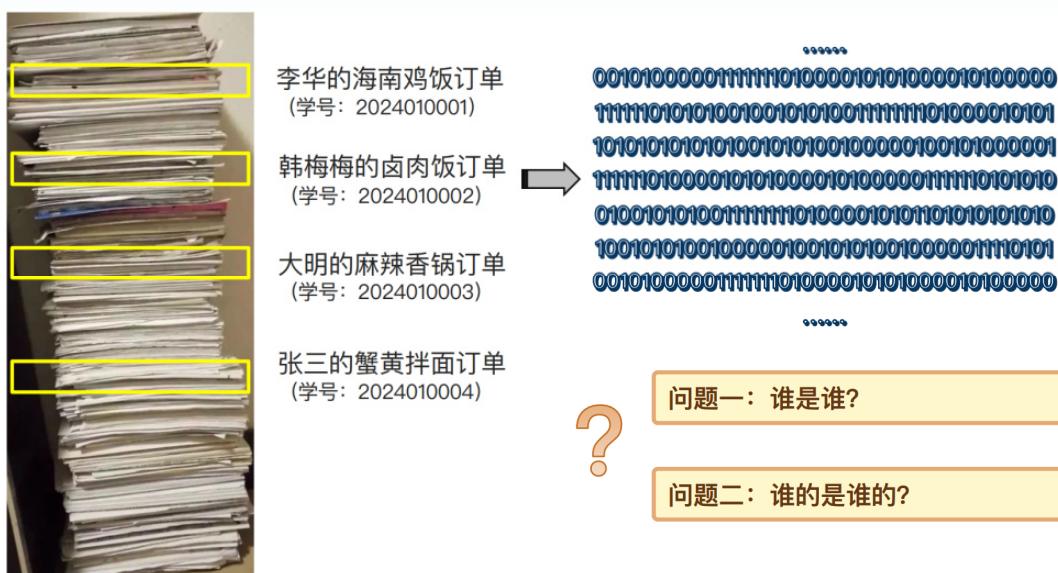


陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

26



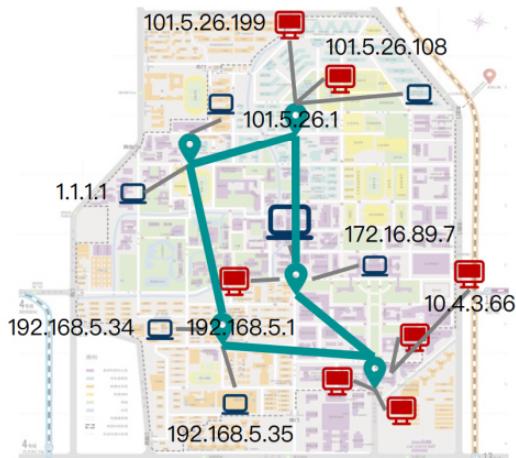
## 如何区分计算机网络中传输的大量内容？



# 如何区分计算机网络中传输的大量内容？

问题一：谁是谁——如何区分网络中的每个设备？

解决方案：为网络中的每个设备分配地址（address）



IP地址：网络设备的“身份证”

- 一般在接入网络后自动分配
- 每个接入网络的设备（包括终端和交换设备）均需要有，否则无法进行数据交换

IP地址的书写形式（IPv4版本）

由四个0-255之间的十进制数组成，数字之间用点号分隔

网络连接详细信息(D):	
属性	值
连接特定的 DNS 后缀	Realtek Gaming GbE Family Controller
描述	E0-D5-5E-8C-AA-98
物理地址	
已启用 DHCP	是
IPv4 地址	192.168.0.92
IPv4 子网掩码	255.255.255.0

29

# 如何区分计算机网络中传输的大量内容？

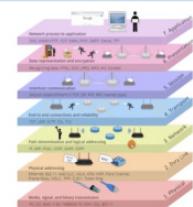
问题二：谁的是谁的——如何确定消息的边界、格式和含义？

解决方案：事先制定网络软硬件遵循的协议（protocol），作为共同的“约定”和“语言”

来源：李华 2024010001	目的：紫荆园
时间：2024年12月16日 12:00	字数：30
内容：	
“我想点【一份海南鸡饭加一杯酸梅汤】 【多加酱油不要香菜】，请送到【教学楼】”	



应用层（外卖）  
软件的消息编码



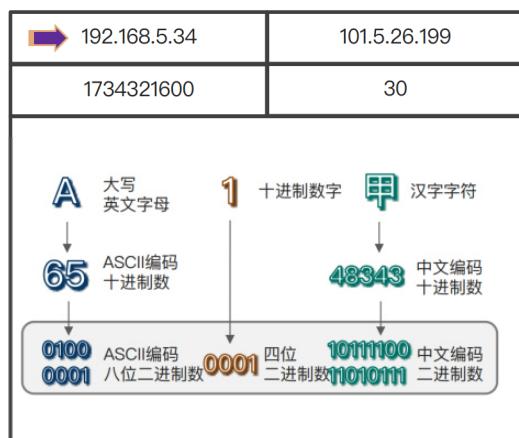
传输层、网络层  
及以下的协议封装

30

# 如何区分计算机网络中传输的大量内容？

问题二：谁的是谁的——如何确定消息的边界、格式和含义？

解决方案：事先制定网络软硬件遵循的协议（protocol），作为共同的“约定”和“语言”



应用层（外卖）  
软件的消息编码



传输层、网络层  
及以下的协议封装

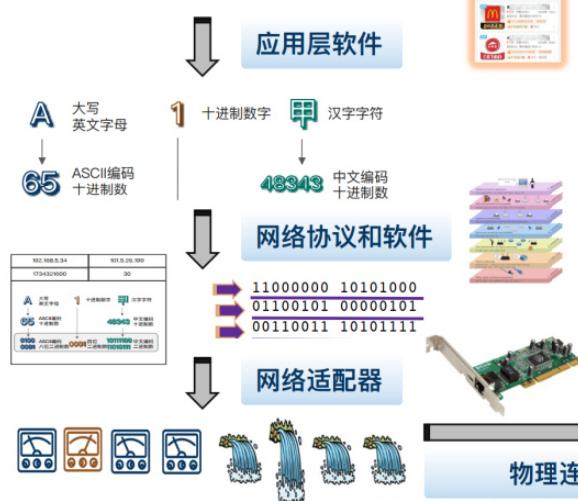
11000000 10101000 00000101 00100010  
01100101 00000101 00011010 11000111  
00110011 10101111 10100101 11000000  
00011110 ..... .... ....  
01000001 00000001 10111100 11010111

31

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 小结：计算机网络中的消息传播路径

“我想点【一份海南鸡饭加一杯酸梅汤】  
【多加酱油不要香菜】，请送到【教学楼】”



“我想点【一份海南鸡饭加一杯酸梅汤】  
【多加酱油不要香菜】，请送到【教学楼】”



陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

32

# 常见的计算机网络应用：网页浏览

将文字、图片、视频等多种信息编码成页面，在浏览器中呈现丰富的显示效果



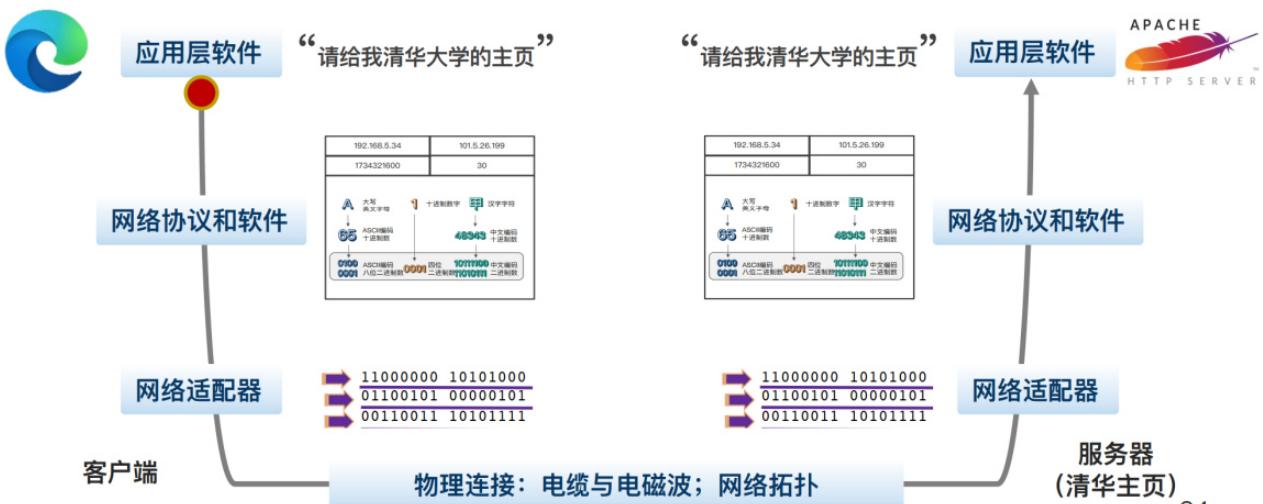
浏览器（应用层软件）  
常见的品牌

33

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

# 常见的计算机网络应用：网页浏览

阶段一：客户端请求 (request)



陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

34

## 常见的计算机网络应用：网页浏览

### 阶段二：服务器响应 (response)



## 常见的计算机网络应用：网页浏览

“我想查看清华大学主页上的校历”

**182.61.200.6**

百度搜索主页的  
服务器IP地址

**162.105.131.160**

北京大学主页的  
服务器IP地址

**101.6.15.66**

清华大学主页的  
服务器IP地址

**问题：不方便记忆**

IP地址的数字没有语义，无法直接  
和对应的机构产生联系

## 常见的计算机网络应用：网页浏览

“我想查看清华大学主页上的校历”

域名 (domain name) : 识别和定位计算机的字符标识



统一资源定位符 (uniform resource locator, URL) : 识别和定位网络上各种类型的具体资源

<https://www.tsinghua.edu.cn/zjqh/syxx/qhxl.htm>

网页浏览  
协议

清华大学主页服务

“走进清华”“实用信息”“清华校历”所在网页

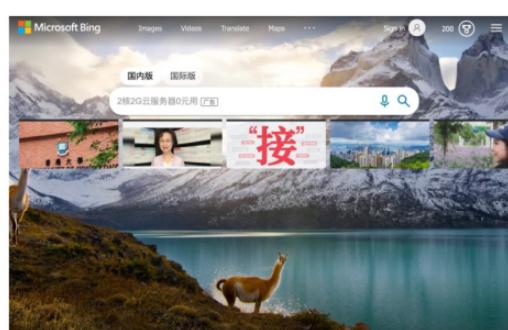
首页 · 走进清华 · 实用信息 · 清华校历

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

37

## 常见的计算机网络应用：搜索引擎

通过关键字搜索海量公开的网页信息



思考：

搜索引擎本身是网页吗？

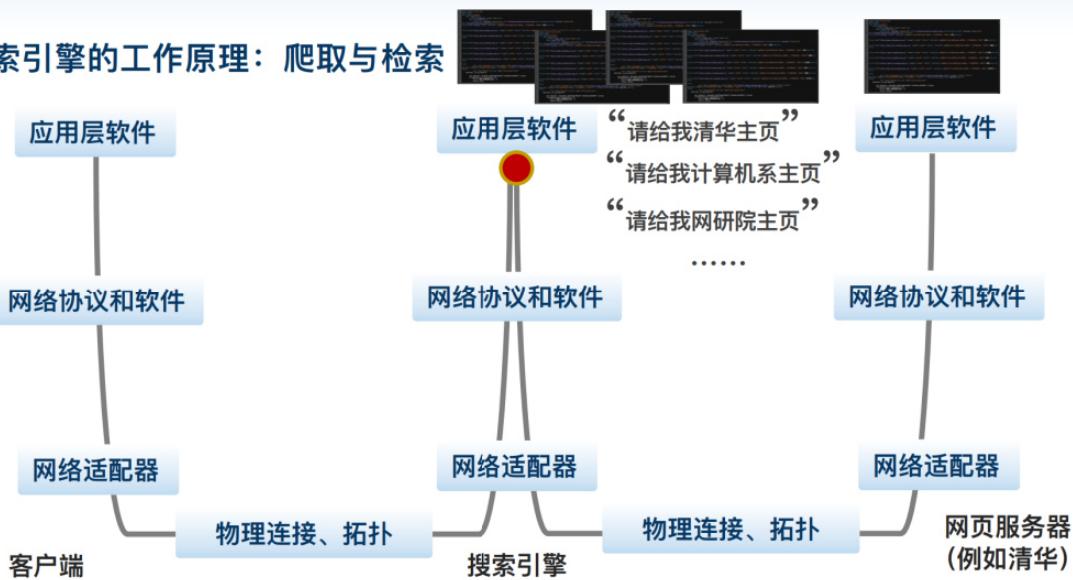
为什么搜索引擎可以很快地帮我们找到想要的信息？

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

38

## 常见的计算机网络应用：搜索引擎

搜索引擎的工作原理：爬取与检索

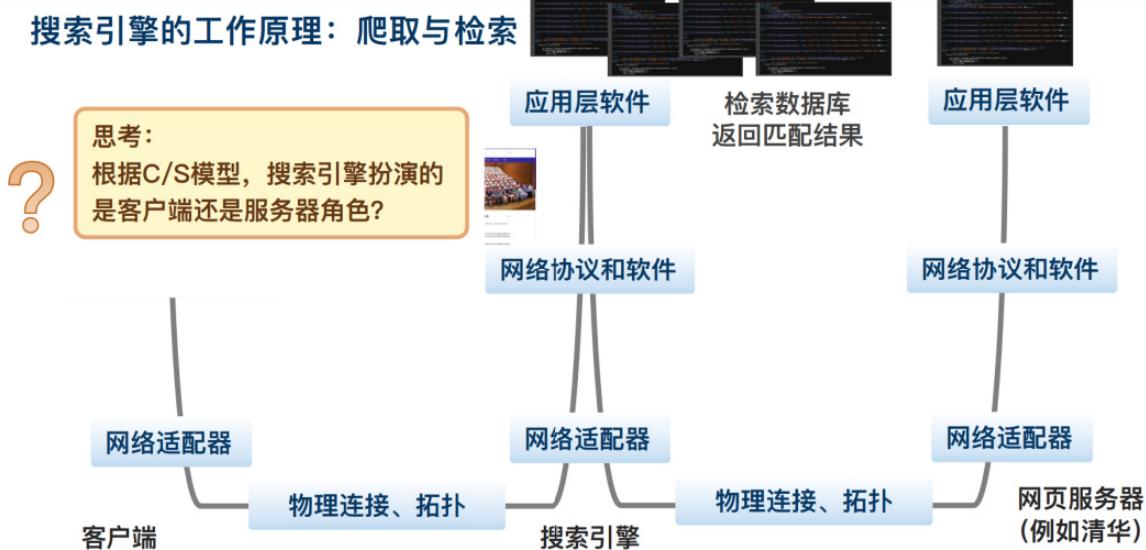


39

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 常见的计算机网络应用：搜索引擎

搜索引擎的工作原理：爬取与检索



40

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

# 常见的计算机网络应用：搜索引擎

## 搜索引擎的工作原理：爬取与检索

思考：

根据C/S模型，搜索引擎扮演的是客户端还是服务器角色？

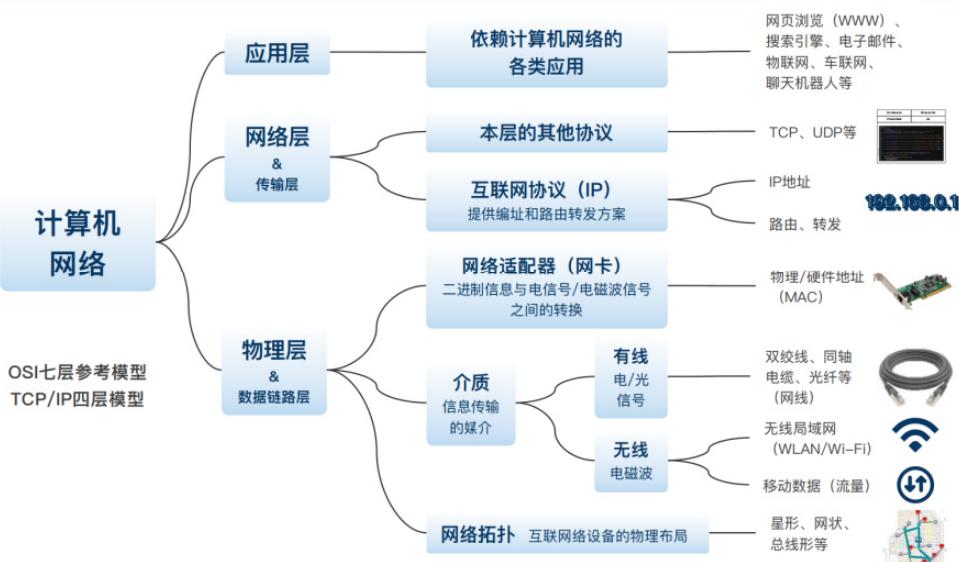
思考：

根据工作原理，为什么对于同样的关键词，不同的搜索引擎返回的结果和排序不完全一样？

### “清华大学计算机系”的搜索结果

41

# 小结：计算机网络体系结构



陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

42

**中场休息，请回顾：**

计算机网络的作用是什么？

计算机网络的组织，需要借助哪些硬件和设备？

什么是协议和IP地址？它们的作用分别是？

你经常使用的互联网应用都有哪些？



课堂意见反馈问卷  
欢迎同学们留下意见建议！

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

43

## 第二部分 Part II

# 网络空间安全引论

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

44

# 你的“外卖” 可能会以什么方式送错甚至丢失?

46

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

信息沿计算机网络传播  
哪些环节可能出问题?

## 一、系统安全

端系统  
软硬件故障  
或遭受威胁

## 二、网络安全

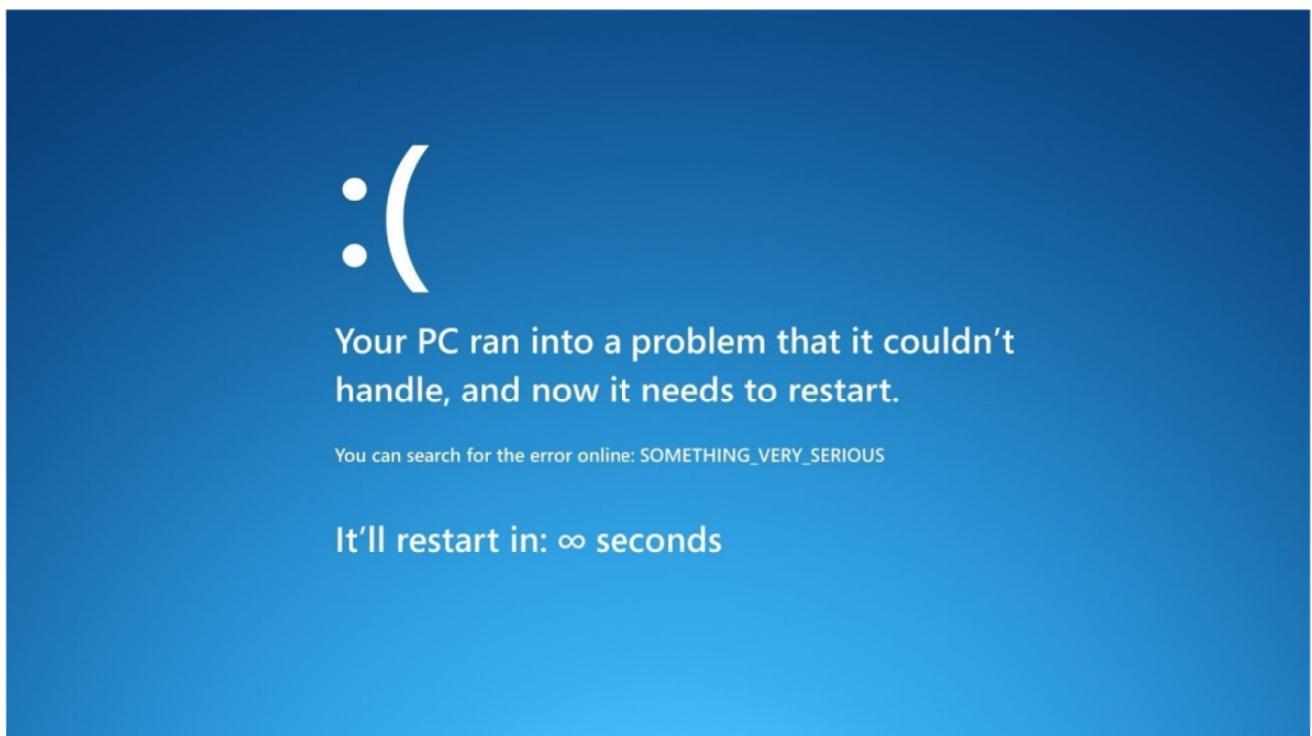
借助信息传输路径  
产生的  
故障或威胁

## 三、应用安全

运行在计算机网络的  
上层应用  
出现非预期行为或  
遭受威胁



47



## 网络空间安全范畴（1）：系统安全

系统安全问题：端系统软硬件发生非预期故障或遭受人为威胁

案例一：系统或软硬件崩溃



操作系统报错蓝屏



手机“刷机”失败  
导致无法正常开机

（俗称“变砖”）

# 网络空间安全范畴（1）：系统安全

系统安全问题：端系统软硬件发生非预期故障或遭受人为威胁

## 案例一：系统或软硬件崩溃



操作系统报错蓝屏



手机“刷机”失败  
导致无法正常开机  
(俗称“变砖”)

## 案例二：软件漏洞挖掘与利用

```
void f (int flag) {  
    char * buf = malloc(100); //mem-leak bug  
    if (flag > 1) {  
        my_free (flag, buf);  
        if (flag > 10)  
            buf = malloc(100); // mem-leak bug  
    }  
    *buf = 0;  
}
```

软件编写时产生的疏漏  
或  
编程语言中的固有缺陷



及时安装更新  
或软件“补丁”  
修复漏洞

50

# 网络空间安全范畴（1）：系统安全

为什么要远离“盗版软件”？

看似省下一笔钱，但背后的代价可能有哪些？

项目	正版软件	盗版软件
侵权 法律责任	风险低	存在 法律风险
分发渠道	正规渠道 (知名应用商店、官方 软件安装包等)	个人分发 来源不明
安装包校验	软件数字签名保障	无校验保障
软件篡改或 非法植入病毒	风险低	存在篡改或 植入可能
软件更新或 安全补丁	存在保障	无更新保障

51CTO 内容精选 视频 话题 短视频 技术期刊 活动

首例微软针对中国大企业盗版案宣判 赔偿217万

sina 新浪财经 产经 > 正文

因使用盗版软件 微软向华创证券索赔842万元！

Win7停更，网络安全风险有多大

澎湃 政务：网信玉田 2020-03-08 22:08

编者按

美国微软公司1月14日宣告Windows 7系统停止更新，官方停止技术支持、软件更新和安全问题的修复，国内网络安全企业360公司15日就披露，一场复合利用IE浏览器和火狐浏览器两个漏洞的攻击风暴悄然突袭，这意味着国内多达六成、仍在使用Windows 7系统的电脑用户无法从微软官方获得支持，将直面各类利用漏洞等威胁进行的攻击。

51

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

# 网络空间安全范畴（1）：系统安全

## 学校向在校师生提供免费校园正版软件

The screenshot shows the Tsinghua University Information Portal homepage. A red arrow points from the 'Software Download' link in the top navigation bar to the 'Public Software' section of the 'Network Information Services' menu. Below this, another red arrow points from the 'Public Software' link to the 'Campus Public Software Download and Installation' section. The page displays various software download links, including Microsoft Visual Studio, MS SQLServer, and Matlab.

类别	软件
操作系统	Windows 10、Windows 11
防病毒软件	NOD32、卡巴斯基
开发软件	MS Visual Studio、MS SQLServer等
办公软件	MS Office、WPS、Foxit PDF编辑器等
计算类软件	Matlab等
其他软件	Adobe等

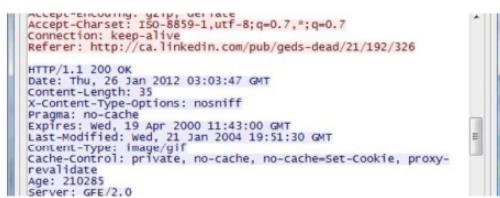
52

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

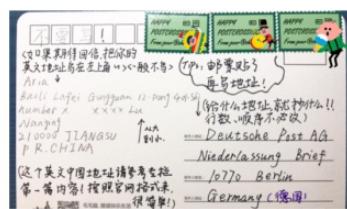
# 网络空间安全范畴（2）：网络安全

## 网络安全问题：借助信息传输路径产生的故障或威胁

### 案例一：通信内容的劫持篡改



### 采用明文传输模式的网络协议（如DNS、HTTP）



网络中的  
“明信片”

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

54

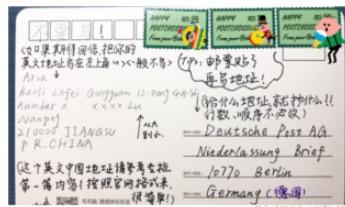
## 网络空间安全范畴（2）：网络安全

### 网络安全问题：借助信息传输路径产生的故障或威胁

#### 案例一：通信内容的劫持篡改

```
HTTP/1.1 200 OK
Date: Thu, 26 Jan 2012 03:03:47 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 33
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Content-Language: zh-CN
Content-Encoding: gzip
Referer: http://ca.linkedin.com/pub/geds-dead/21/192/326
Pragma: no-Cache
Expires: wed, 19 Apr 2000 11:43:00 GMT
Last-Modified: wed, 21 Jan 2004 19:51:30 GMT
Content-Type: application/x-gzip
Cache-Control: private, no-cache, no-cache-set-cookie, proxy-revalidate
Age: 210285
Server: GFE/2.0
```

采用明文传输模式的网络协议（如DNS、HTTP）



网络中的  
“明信片”



百度搜索主页遭劫持（2010年）

浏览网页被注入广告

#### 腾讯等六家互联网公司联合声明：抵制流量劫持

-2015-  
12/25 【环球科技报道 周涛】今日，今日头条、美团大众点评网、360、腾讯、微博、小米科技等六家互联网公司联合表达共同诉求：呼吁有关运营商严厉打击流量劫持问题，并保留进一步采取联合行动的可能。  
10:33

55

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（2）：网络安全

### 网络安全问题：借助信息传输路径产生的故障或威胁

#### 案例二：计算机病毒

##### 木马（Trojan）：用于远程控制受害计算机的程序

以隐蔽的方式进入目标机器，根据远程攻击者下达的指令，获取权限、收集信息及执行恶意代码

58

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（2）：网络安全

网络安全问题：借助信息传输路径产生的故障或威胁

### 案例二：计算机病毒

木马（Trojan）：用于远程控制受害计算机的程序

以隐蔽的方式进入目标机器，根据远程攻击者下达的指令，获取权限、收集信息及执行恶意代码



59

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（2）：网络安全

网络安全问题：借助信息传输路径产生的故障或威胁

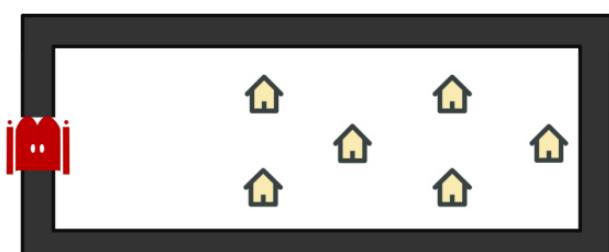
### 案例二：计算机病毒

木马（Trojan）：用于远程控制受害计算机的程序

以隐蔽的方式进入目标机器，根据远程攻击者下达的指令，获取权限、收集信息及执行恶意代码



不打了？  
撤军了？



60

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

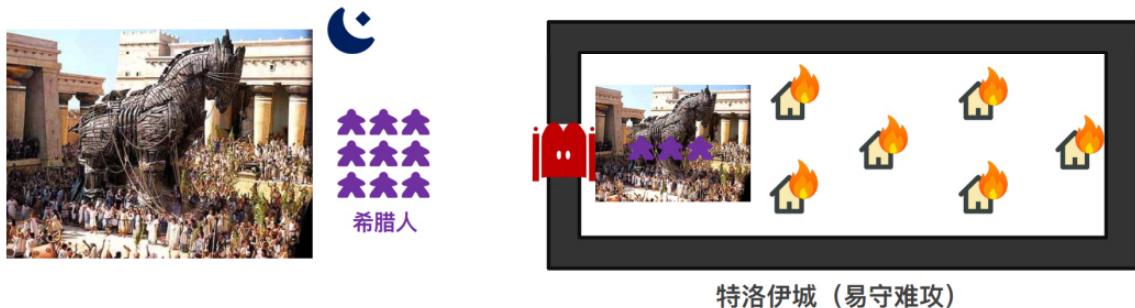
## 网络空间安全范畴（2）：网络安全

网络安全问题：借助信息传输路径产生的故障或威胁

### 案例二：计算机病毒

木马（Trojan）：用于远程控制受害计算机的程序

以隐蔽的方式进入目标机器，根据远程攻击者下达的指令，获取权限、收集信息及执行恶意代码



61

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

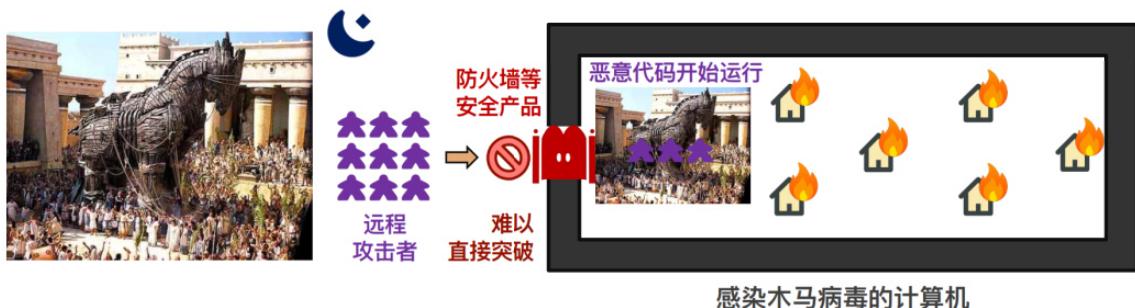
## 网络空间安全范畴（2）：网络安全

网络安全问题：借助信息传输路径产生的故障或威胁

### 案例二：计算机病毒

木马（Trojan）：用于远程控制受害计算机的程序

以隐蔽的方式进入目标机器，根据远程攻击者下达的指令，获取权限、收集信息及执行恶意代码



62

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（2）：网络安全

小心“引马入室”：为什么要警惕来路不明的网站、链接、二维码？



陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

63

## 网络空间安全范畴（2）：网络安全

小心“引马入室”：为什么要警惕来路不明的公共Wi-Fi、充电宝（数据线）？



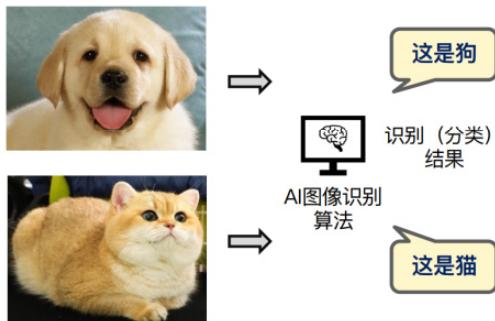
陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

64

## 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

### 案例一：图像识别算法安全



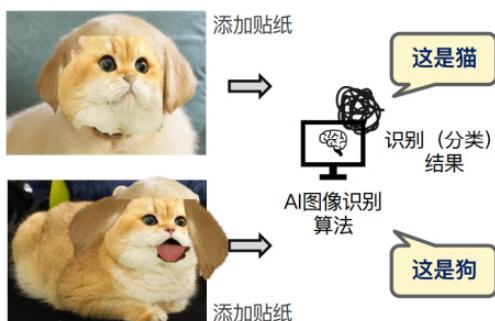
66

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

### 案例一：图像识别算法安全



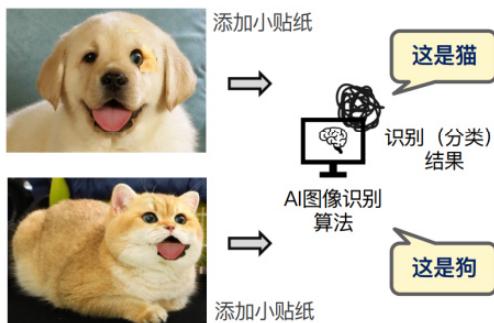
67

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

### 案例一：图像识别算法安全



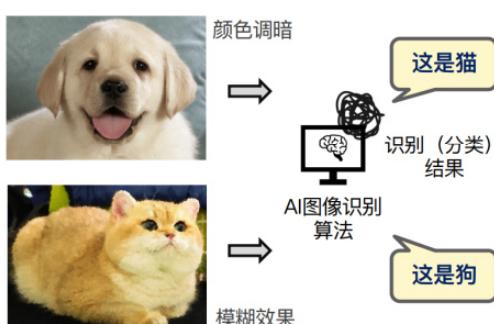
68

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

### 案例一：图像识别算法安全



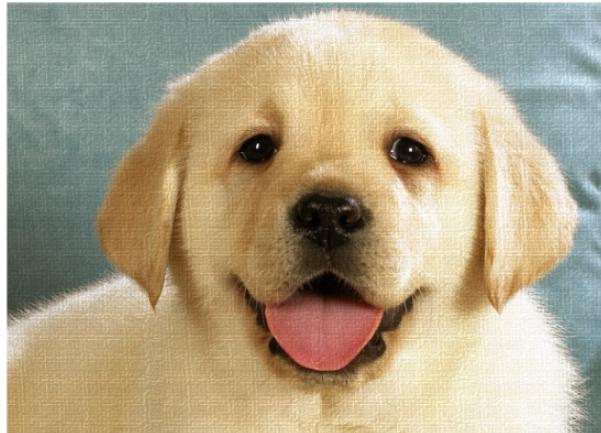
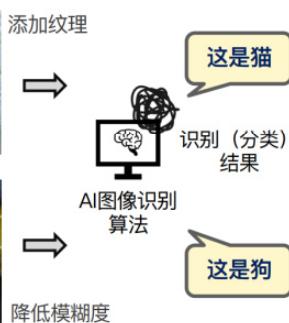
69

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

### 案例一：图像识别算法安全



#### 对抗样本（Adversarial examples）

在数据集中故意添加细微的干扰

导致模型以高置信度给出错误的输出

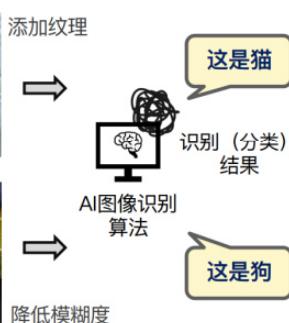
陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

70

## 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

### 案例一：图像识别算法安全



自动驾驶算法对路况和交通标志的识别



通过  
形变、磨损、遮挡  
形成对抗样本

#### 对抗样本（Adversarial examples）

在数据集中故意添加细微的干扰

导致模型以高置信度给出错误的输出

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

71

## 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

### 案例二：大语言模型（Large Language Model, LLM）安全



#### 大模型幻觉 (hallucination)

由于模型数据、训练过程中的错误

导致“一本正经地胡说八道”

#### 提示词 (prompt) 攻击

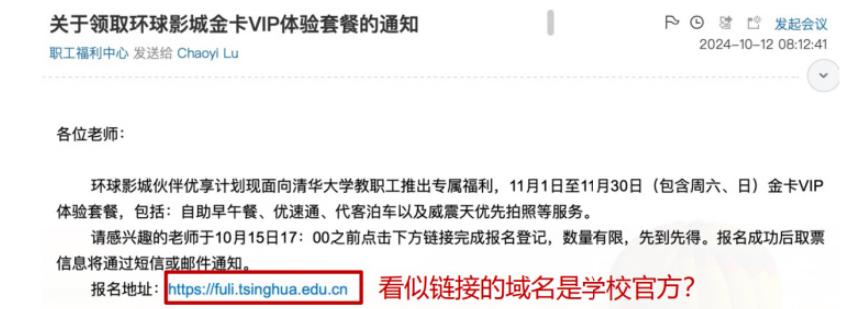
刻意构造输入导致大模型生成不当内容、泄漏信息 72

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

### 案例三：电信网络诈骗、敲诈勒索



# 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

## 案例三：电信网络诈骗、敲诈勒索

### 关于领取环球影城金卡VIP体验套餐的通知

职工福利中心 发送给 Chaoyi Lu



发起会议  
2024-10-12 08:12:41



### 网络钓鱼（Phishing）攻击

通过发送欺骗性信息，诱导受害人给出敏感信息（身份、账号等）的攻击方式

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

74

# 网络空间安全范畴（3）：应用安全

应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

## 案例三：电信网络诈骗、敲诈勒索

### 2024年钓鱼邮件演练工作通报

用户通知 宣传栏 教工邮件列表

各位老师：

您好！为提高师生对钓鱼邮件的识别能力，提升师生网络安全意识，防范化解钓鱼邮件风险隐患，保障学校业务数据和用户个人信息安全，我校于10月12日早8:00至15日下午5:00面向教职工组织开展了钓鱼邮件演练。

本次演练邮件主题为“关于领取环球影城金卡VIP体验套餐的通知”，其中打开钓鱼链接接受培训的用户占比12.2%，输入密码“被钓鱼”的用户占比4.6%。演练未记录账号密码，不会对系统和设备造成影响。以下为您收到的演练邮件样本分析。



### 学校2024年钓鱼邮件演练结果

12.2% 用户打开了邮件中的钓鱼链接

4.6% 用户在打开的页面中输入了校园网账号口令

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

75

## 网络空间安全范畴（3）：应用安全

为什么要警惕“天上掉馅饼”？

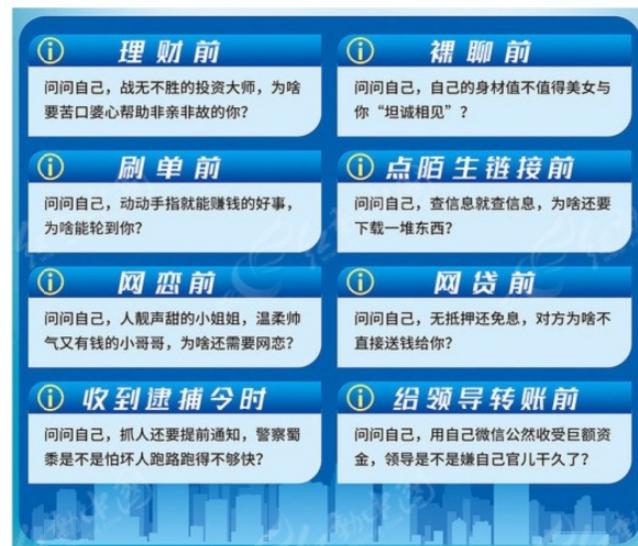
**防骗秘诀“八个凡是”**

\* 心中无贪念 | 骗局远身边 \*

**统统不要相信**

- 凡是自称公检法要求汇款的；
- 凡是叫你汇款到“安全账户”的；
- 凡是通知中奖、领取补贴要你先交钱的；
- 凡是通知“家属”出事要汇款的；
- 凡是在电话中索要银行信息及短信验证码的；
- 凡是让你开通网银接受检查的；
- 凡是自称领导要求打款的；
- 凡是陌生网站要登记银行卡的，

如遇疑似诈骗请拨打  
反诈热线96110



① 理财前  
问问自己，战无不胜的投资大师，为啥要苦口婆心帮助非亲非故的你？

② 裸聊前  
问问自己，自己的身材值不值得美女与你“坦诚相见”？

③ 刷单前  
问问自己，动动手指就能赚钱的好事，为啥轮到你？

④ 点陌生链接前  
问问自己，查信息就查信息，为啥还要下载一堆东西？

⑤ 网恋前  
问问自己，人靓声甜的小姐姐，温柔帅气又有钱的小哥哥，为啥还需要网恋？

⑥ 网贷前  
问问自己，无抵押还免息，对方为啥不直接送钱给你？

⑦ 收到逮捕令时  
问问自己，抓人还要提前通知，警察蜀黍是不是怕坏人跑路跑得不够快？

⑧ 给领导转账前  
问问自己，用自己微信公然收受巨额资金，领导是不是嫌自己官儿干久了？

76

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（4）：密码学及应用

密码学及应用：为网络空间安全各类应用提供基础性支撑

**案例一：加密网络通信（保密性）**

传输的内容不再对网络中间设备可见



```
HTTP/1.1 200 OK
Date: Thu, 26 Jan 2012 03:03:47 GMT
Content-Length: 35
X-Content-Type-Options: nosniff
Pragma: no-cache
Expires: Sat, 19 Apr 2000 11:43:00 GMT
Last-Modified: Wed, 21 Jan 2004 19:51:30 GMT
Content-Type: image/gif
Cache-Control: private, no-cache, no-cache=Set-cookie, proxy-revalidate
Age: 210285
Server: GFE/2.0
```

加密 (encrypt) ↓      ↑ 解密 (decrypt)

```
.....H..  
.....0..  
.....e$^.B..p....29].$.K0.$x.....r.3\|t.0..T.b...nk-.P.t...  
7.....&....H..  
..z...SK.....:..R...r/.....,X.....r....bX.^k....Wj...T  
***  
.....7.'!^..q0...f...g...z...*.M.!....q....}..f..  
WQ4...a...+.+..aUU..}..UM..O..yN.q.*f...fn..G....b6...[....[x..]2]M.F.  
7.....q...r....HvY..C.....@+..9...  
8\+..}8.h...".M.....{.y...S....V...F...vt.a....  
7*VD.F.r....P...a...q....Q  
N 1 5 3  *  f  o  r  d  Rn
```

78

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（4）：密码学及应用

密码学及应用：为网络空间安全各类应用提供基础性支撑

#### 案例一：加密网络通信（保密性）

传输的内容不再对网络中间设备可见

HTTP/1.1 200 OK  
Date: Thu, 26 Jan 2012 03:03:47 GMT  
Content-Type: text/html; charset=gbk  
X-Content-Type-Options: nosniff  
Pragma: no-cache  
Expires: Wed, 19 Apr 2000 11:43:00 GMT  
Last-Modified: Wed, 21 Jan 2004 19:51:30 GMT  
Content-Type: image/gif  
Cache-Control: private, no-cache, no-cache=set-cookie, proxy-revalidate  
Age: 210285  
Server: GFE/2.0

加密 (encrypt)   解密 (decrypt)

. . \*..H..  
. ....B..  
. ....t..e\$....B..p.....29]\$.KO.\$x.....r.3\|t\0..T.b...nk-..P.t...  
7....8....H..  
z....SK|.....:....R..r/.....X.....r..r..bx.^kj..Wj..^T  
....  
.... 7..!..0@.....f..g..z..\*.....M..!..l..q..}..f..  
WQ4....a....+..,+allU..]Um..0..yhl..q..+..f../\n..G..b6..[....|x..]2.M.F.  
....q..r..q..HvY..C..@..+,9....  
8V+....8..h..-..M..(....y..S....V..F..vt.a....  
7\*VD..F..r..P..m..q....Q  
N .. 1 .. 2 .. 3 .. 4 .. 5 .. 6 .. 7 .. 8 .. 9 .. 0 .. R .. S .. T .. U .. V .. W .. X .. Y .. Z ..

## 案例二：数据内容校验（完整性）

检查数据内容或软件是否遭到篡改



79

## 网络空间安全范畴（4）：密码学及应用

密码学及应用：为网络空间安全各类应用提供基础性支撑

#### 案例一：加密网络通信（保密性）

传输的内容不再对网络中间设备可见

Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7  
Connection: keep-alive  
Referer: http://ca.linkedin.com/pub/geds-dead/21/192/326

HTTP/1.1 200 OK  
Date: Thu, 26 Jan 2012 03:03:47 GMT  
Content-Length: 35  
X-Content-Type-Options: nosniff  
Pragma: no-cache  
Expires: Wed, 19 Apr 2000 11:43:00 GMT  
Last-Modified: wed, 21 Jan 2004 19:51:30 GMT  
Content-Type: image/gif  
Cache-Control: private, no-cache, no-cache=set-cookie, proxy-revalidate  
Age: 210285  
Server: GFE/2.0

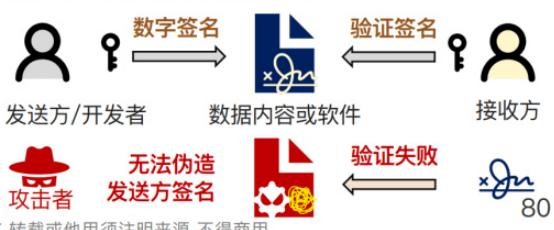
加密 (encrypt)   解密 (decrypt)

. . \*..H..  
.....B..  
....t..e\$...A..p....29]\$.KO.\$x.....r.3t.0..T.b..nk-.P.t...  
7....8...H..  
z..SK|.....:^..R..r/r.....X.....r..bx.^k..Wj..Wj..T  
....  
.... 7..!..q0.....f..g..z.\*.....M.!..q-)...f...  
WQ4....a...+..,+allU\_).UM..0..yhl.q..+..f../\n..G...b6...[...x]2M.F.  
8V..)8..q..r..HvY..C..@..,.9.....  
8V..)8..q..r..HvY..C..@..,.9.....  
7\*WD..F.r..Pm..q...Q  
N .. 1 .. 5 .. 3 .. 6 .. O .. 8 .. R .. 9 ..

大陆联通 清华大学网络研究院 版权所有

## 案例二：数据内容校验（完整性）

检查数据内容或软件是否遭到篡改



80

## 网络空间安全范畴（4）：密码学及应用

生活中这些“密码”，是真正的密码吗？



**密码 (Cryptography)**：对原始数据进行加解密运算，用于保障机密性、完整性、可用性

**口令 (Password)**：用于身份认证（通信双方之间的“暗号”）

81

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全范畴（4）：密码学及应用

为什么不要设置“弱口令”？

**特征一：长度过短**

长度越短，暴力破解所需尝试次数越低

例：由小写英文字母组成口令，每秒尝试100次

6位长度 3亿种组合 一个月破解

10位长度 100万亿种组合 两万年破解

**特征二：组成过于简单**

组成简单，暴力破解所需尝试次数越低

例：6位口令，每秒尝试100次

纯小写字母 3亿种组合 一个月破解

大小写混合 190亿种组合 五年破解

字母混合+数字 560亿种组合 十五年破解

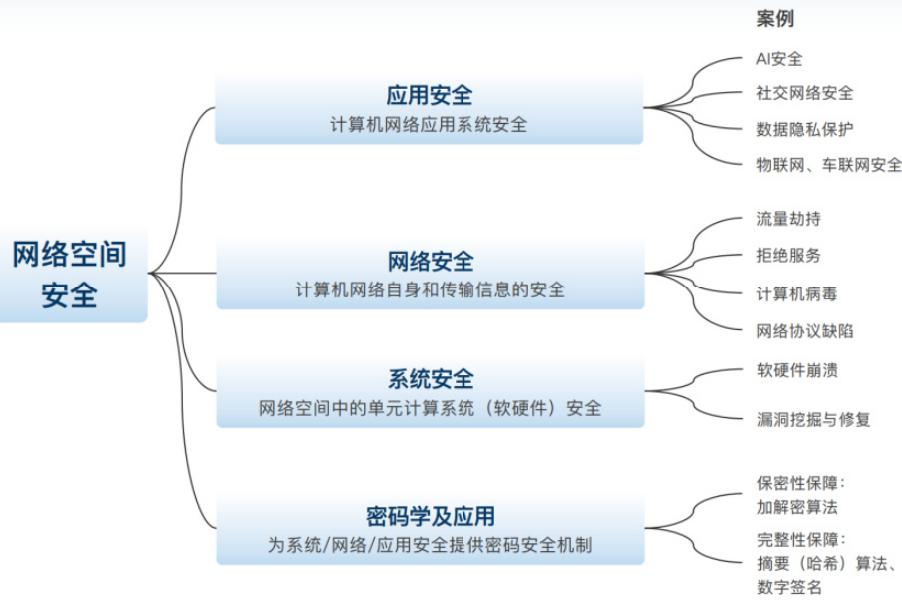


**特征三：和容易联想到的个人或公开信息相关**  
例如生日、物品名称、键盘组合等

82

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 小结：网络空间安全



83

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

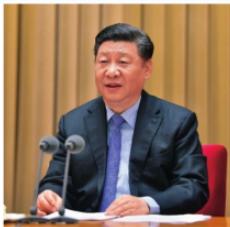
## 第三部分 Part III

# 网络空间安全的国家战略地位

84

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

## 网络空间安全的国家战略地位



“没有网络安全就没有国家安全，没有信息化就没有现代化。”

——2014年2月27日，习近平在中央网络安全和信息化领导小组第一次会议上发表讲话



### 《中华人民共和国网络安全法》

2016年11月7日  
第十二届全国人民代表大会常务委员会第二十四次会议通过



### 《国家网络空间安全战略》

2016年12月27日  
国家互联网信息办公室发布  
制定了捍卫网络空间主权等9个方面的战略任务

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

85

## 网络空间安全相关部署与行动

### 全国范围内统一开展“国家网络安全宣传周”主题活动

由中宣部、中央网信办等部门联合举办，每年举办一届

届别	主题
第一、二届	“共建网络安全，共享网络文明”
第三至十一届	“网络安全为人民，网络安全靠人民”



主旨论坛与博览会



网络安全赛事



网络安全宣传微视频

86

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

# 网络空间安全相关部署与行动

## “全民反诈在行动”防范电信网络诈骗犯罪活动

由中宣部、公安部联合部署，2024年主题为“警惕诈骗新手法，不做电诈工具人”



87

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

# “网络空间安全”一级学科

## 增设“网络空间安全”一级学科，加快高层次人才培养



2015年6月，经国务院学位委员会批准  
增设“网络空间安全”一级学科



“网络空间的竞争，归根结底是人才竞争。”  
“人才是网络安全第一资源。”

2016年6月，中央网信办等六部门联合发布  
关于加强网络安全学科建设和人才培养的意见

88

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

# “网络空间安全”一级学科

研究对象：网络空间中的安全威胁和防护问题

基础设施、信息系统的安全和可信；信息的保密性、完整性、可用性、真实性和可控性等相关理论和技术



## 清华大学网络空间安全学科培养方案（由网络研究院承担）



陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用

89

计算机网络与网络空间安全  
欢迎对本次课堂提出宝贵意见！

陆超逸

清华大学 网络科学与网络空间研究院 博士后

电子邮箱：[luchaoyi@tsinghua.edu.cn](mailto:luchaoyi@tsinghua.edu.cn)

个人主页：<https://chaoyi.lu>

2024年12月



课堂意见反馈问卷  
(真的是问卷星，不是有害网站)  
下课过后不要乱扫别的二维码啊！

陆超逸 清华大学网络研究院 版权归作者所有 转载或他用须注明来源 不得商用