《计算机文化基础》课程

计算机网络与网络空间安全

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

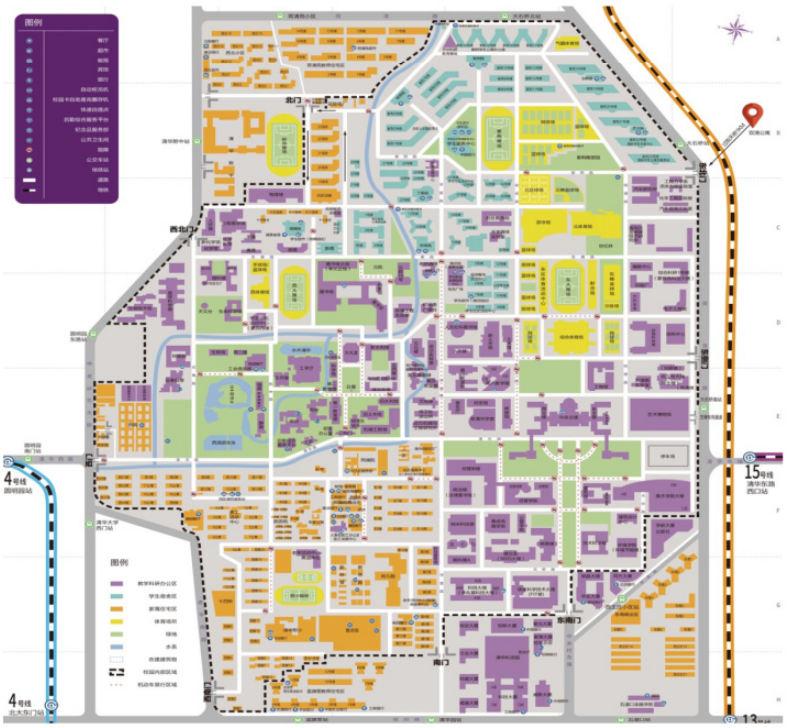
2024年12月

第一部分 Part I

计算机网络引论

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——




麦当劳
精选
美味饭菜
汉堡披萨
奶茶果汁
米粉面馆
全部
综合排序
分类
速度
全部筛选
换一换
天天爆红包
减配送费
无门槛红包
肯
4.9分 月售2000+ 30分钟 481m
起送¥20 满30配送 约¥3
近期买过2次 吮指原味鸡
集点返3元 食无忧 开发票
KFC
炸鸡5拼39.9
麦
4.5分 月售2000+ 30分钟 1.6km
起送¥30 满30配送 约¥3
37人觉得性价比高 收录9年
8件64.9
必
4.7分 月售1000+ 40分钟 594m
起送¥20 满59配送 约¥2
近30日204个回头客 浓情香鸡翼
必胜客
买1送1
德
4.8分 月售1000+ 25分钟 2.9km
起送¥20 免配送费
蜂鸟准时达
近期买过 三拼小食套餐
当前所在地
(教学楼)

5


目标餐厅
麦当劳
精选
美味饭菜
汉堡披萨
奶茶果汁
米粉面馆
全部
综合排序
分类
速度
全部筛选
换一换
天天爆红包
减配送费
无门槛红包
肯
4.9分 月售2000+ 30分钟 481m
起送¥20 满30配送 约¥3
近期买过2次 吮指原味鸡
集点返3元 食无忧 开发票
KFC
炸鸡5拼39.9
麦
4.5分 月售2000+ 30分钟 1.6km
起送¥30 满30配送 约¥3
37人觉得性价比高 收录9年
8件64.9
必
4.7分 月售1000+ 40分钟 594m
起送¥20 满59配送 约¥2
近30日204个回头客 浓情香鸡翼
必胜客
买1送1
德
4.8分 月售1000+ 25分钟 2.9km
起送¥20 免配送费
蜂鸟准时达
近期买过 三拼小食套餐
当前所在地
(教学楼)

6

7

8

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

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

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

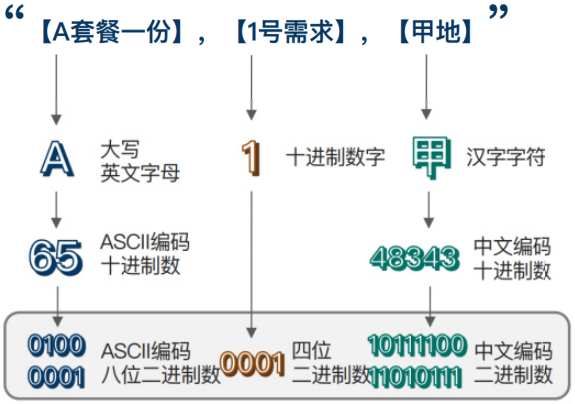
版本2.0
借助计算机的
“点对点”信息传递

借助计算机进行通信
进一步提升效率

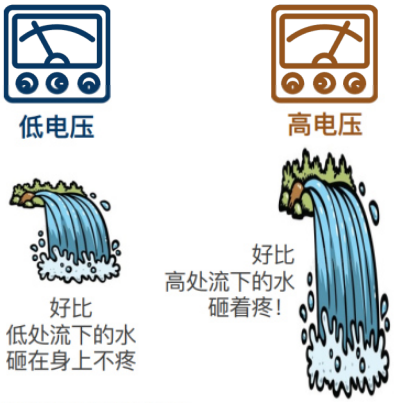
计算机之间的通信介质：电缆与电信号

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？

信息在计算机中使用
二进制（0或1）的形式编码

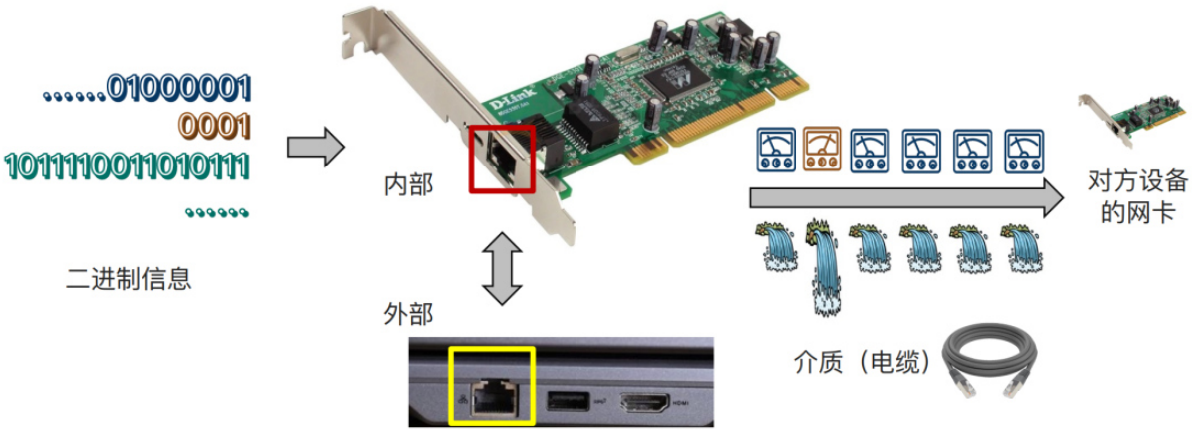


使用电信号可以
较为容易地表示（0或1）两种状态



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



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

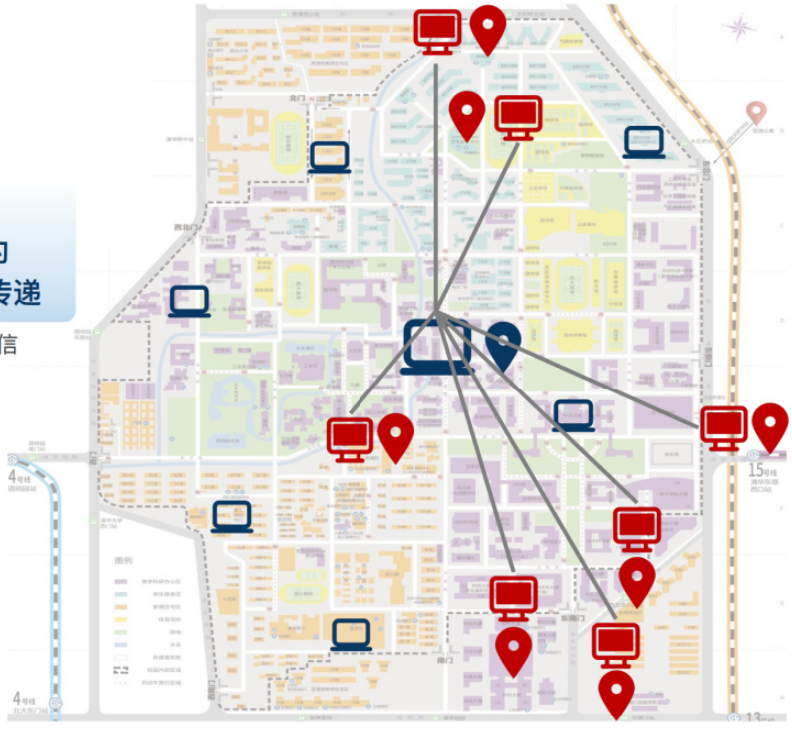
客户端–服务器（C/S）模型

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

思考：
版本2.0在后续发展的过程中，可能会遇到什么问题？

版本2.0
借助计算机的
“点对点”信息传递

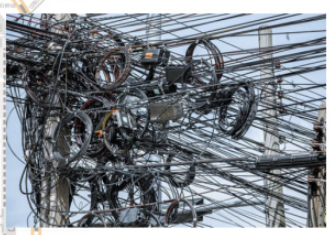
借助计算机进行通信
进一步提升效率



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

存在问题：可扩展性差
采用“专线”，难以满足多个客户端、服务器的场景需求
（即难以实现“互联互通”）



版本3.0
共用信息传输介质
“分而治之”

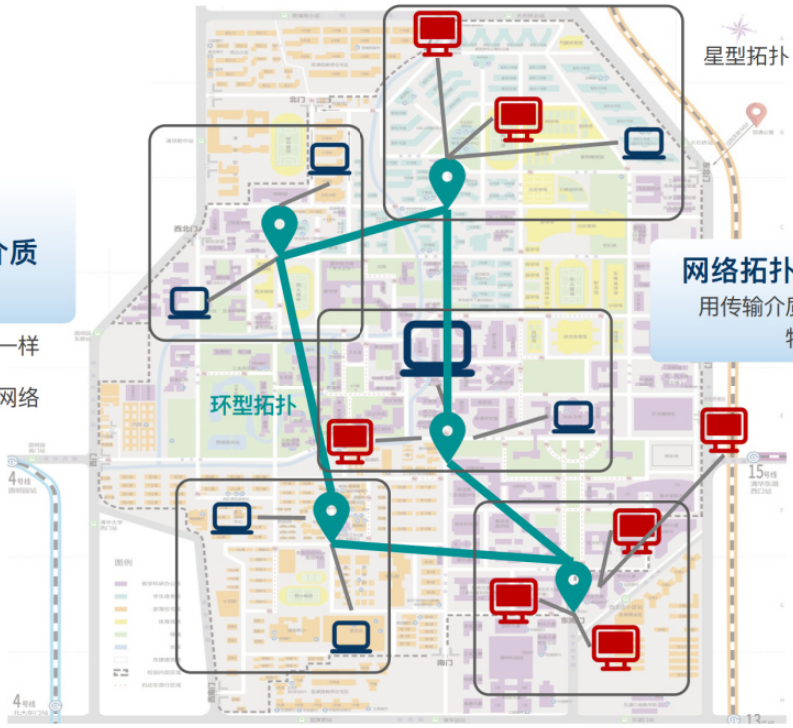
你的电缆我的电缆都一样
构建有组织的
计算机间的信息共享网络

具备可扩展性：
- 端设备加入时接入最近一个“路口”设备即可
- “路口”及其间的线路（绿色）由专人负责架设和运营，通信双方无需考虑

转发（forwarding）
网络设备将数据发往下一个网络设备的过程

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



网络拓扑（topology）
用传输介质互联各种设备的
物理布局

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 | **房间里的** | **楼栋里的** | **地区内的**

计算机

墙面网口

家用路由器

交换机房

大型网络机房

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”

中国电信 CHINA TELECOM

China unicom 中国联通

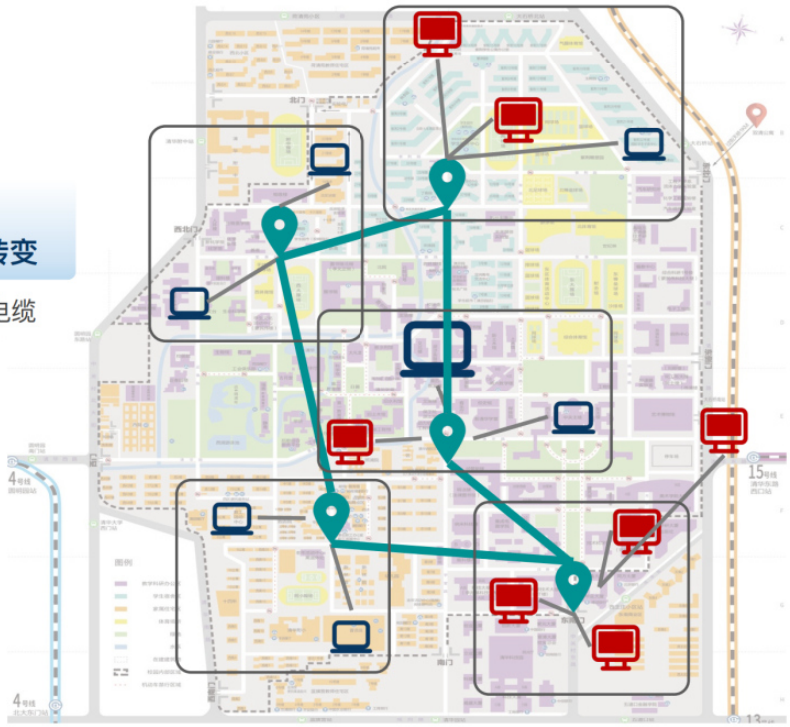
中国移动 China Mobile

中国教育和科研计算机网（CERNET）

CERNET

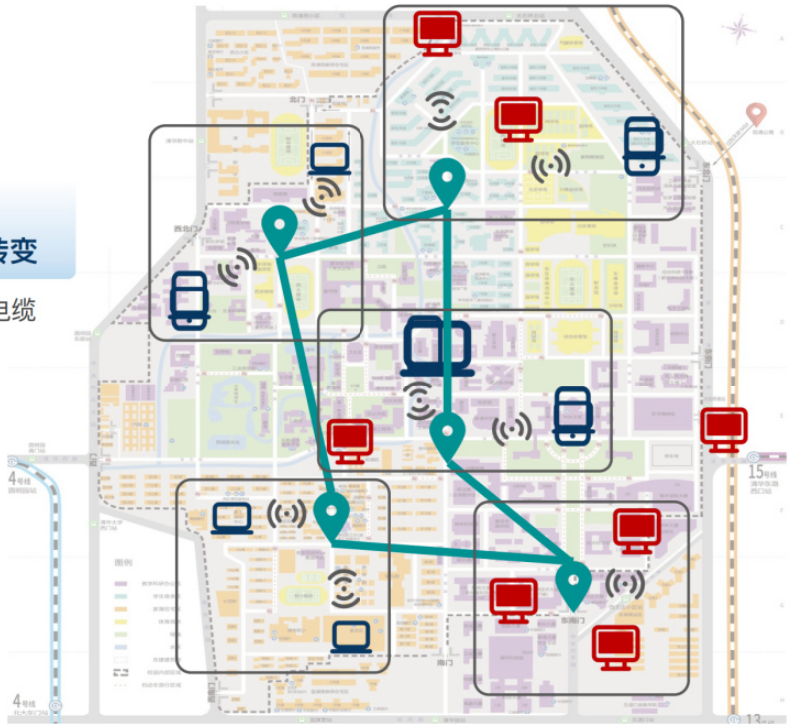
版本3.1
有线向无线的转变

使用电磁波代替电缆
作为传输介质



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



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

计算机上的网口

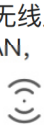
电缆（网线）连接

墙面网口
或
路由器网口

通过无线介质（电磁波）接入

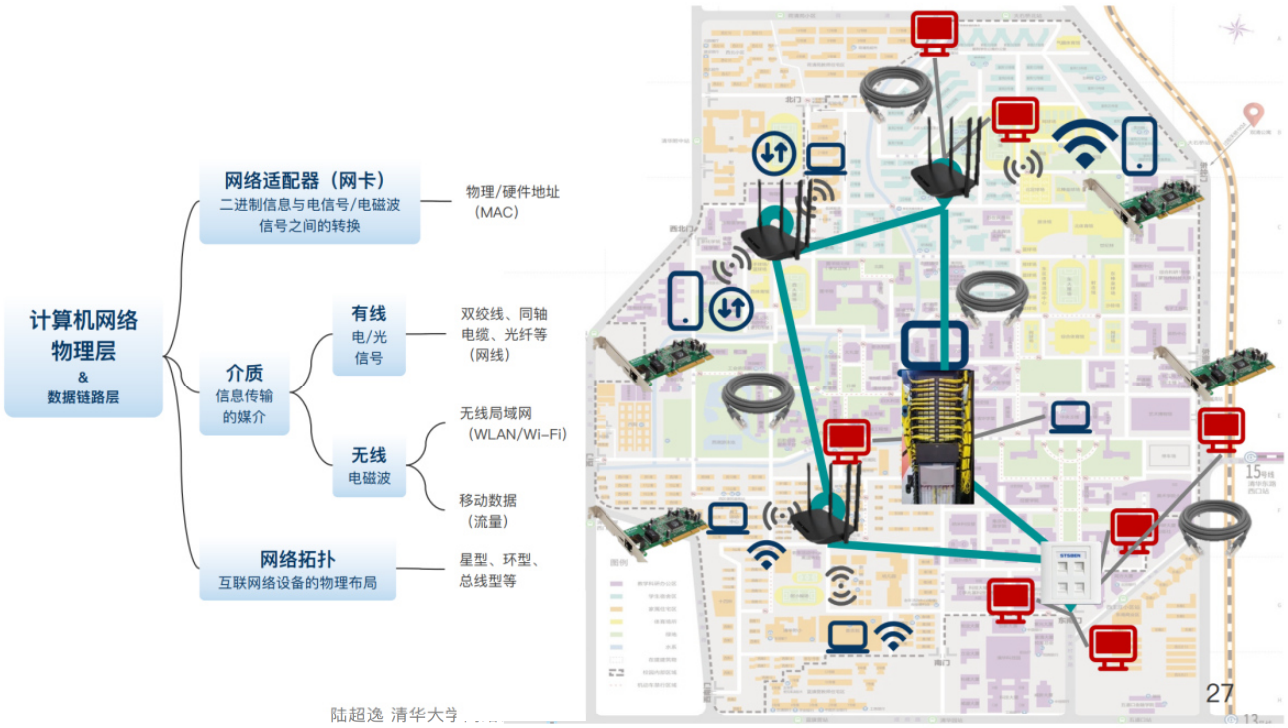
无线局域网
（WLAN，俗称**Wi-Fi**）

移动数据
（俗称**流量**）

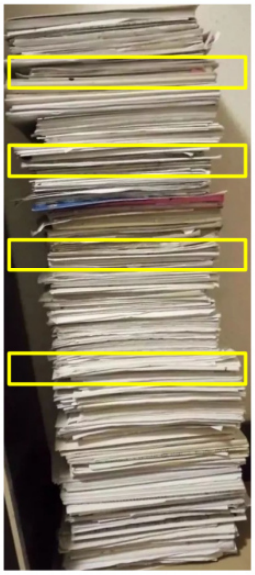


无线路由器（接入点）

通信基站



如何区分计算机网络中传输的大量内容？

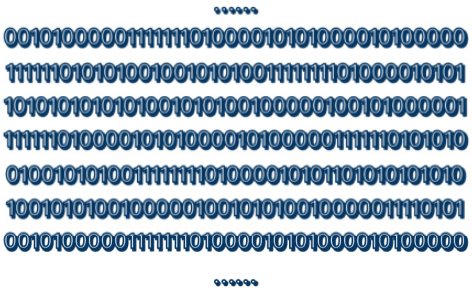


李华的海南鸡饭订单
（学号：2024010001）

韩梅梅的卤肉饭订单
（学号：2024010002）

大明的麻辣香锅订单
（学号：2024010003）

张三的蟹黄拌面订单
（学号：2024010004）



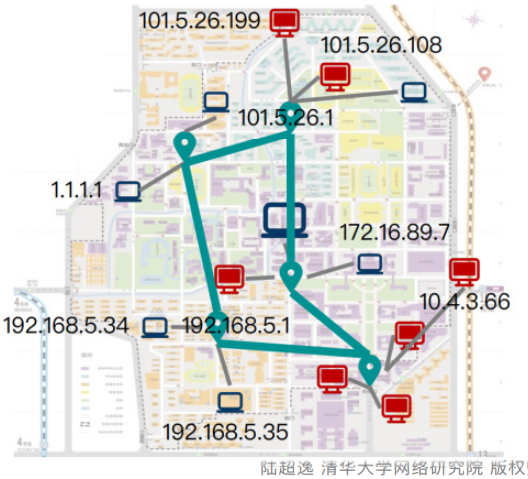
问题一：谁是谁？

问题二：谁的是谁的？

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）

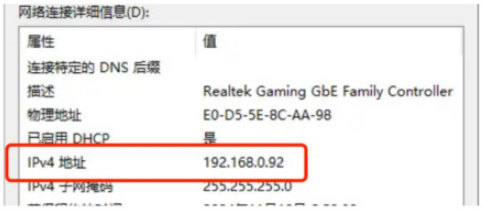


IP地址：网络设备的“身份证”

- 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



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】”	

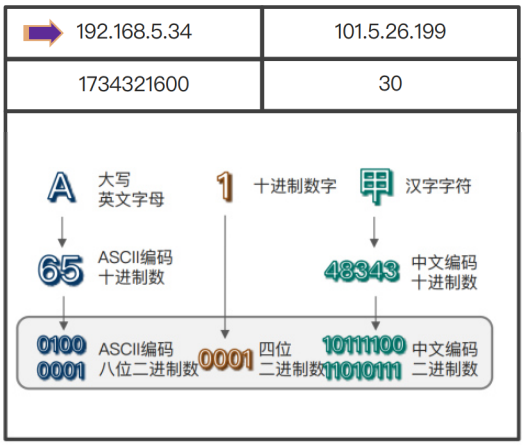
应用层（外卖）软件的消息编码

传输层、网络层及以下的协议封装

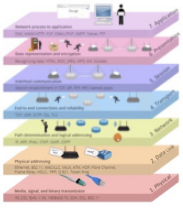
如何区分计算机网络中传输的大量内容？

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
```


小结：计算机网络中的消息传播路径

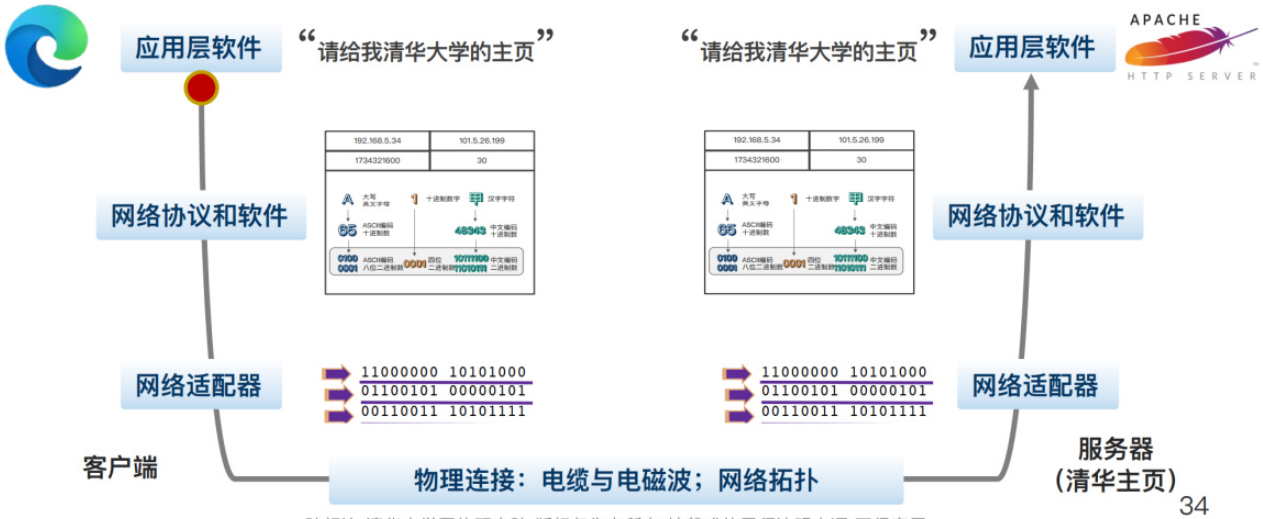
常见的计算机网络应用：网页浏览

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

常见的计算机网络应用：网页浏览

阶段一：客户端请求（request）



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

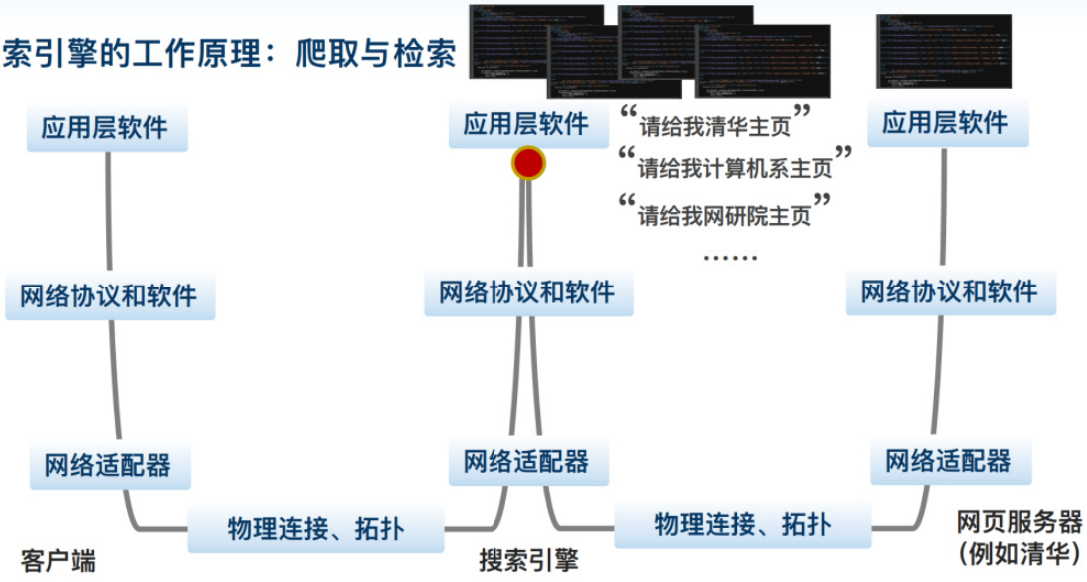
常见的计算机网络应用：搜索引擎

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速地帮我们找到想要的信息？

常见的计算机网络应用：搜索引擎

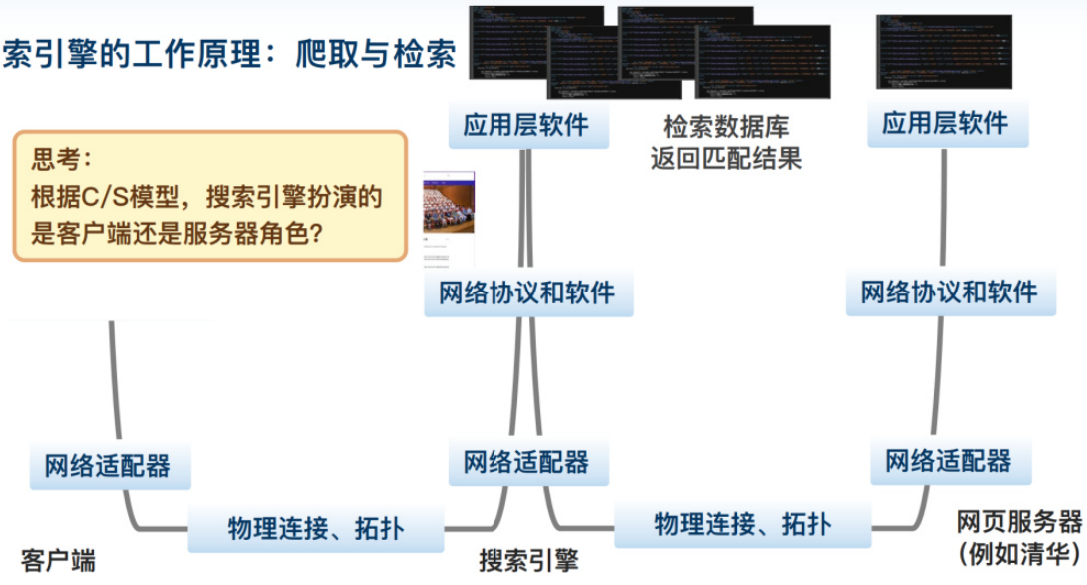
搜索引擎的工作原理：爬取与检索



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?



常见的计算机网络应用：搜索引擎

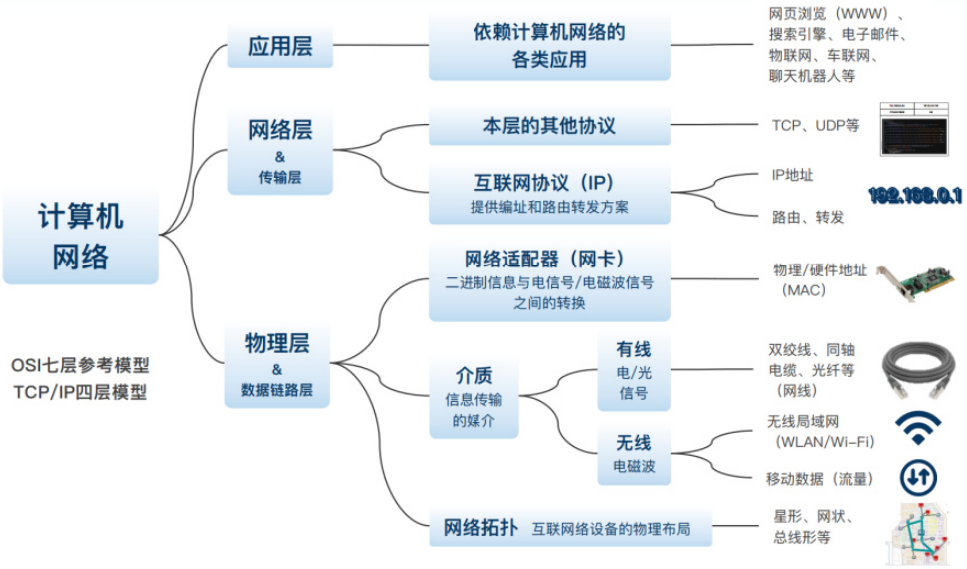
搜索引擎的工作原理：爬取与检索

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

小结：计算机网络体系结构



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！

第二部分 Part II

网络空间安全引论

你的“外卖”
可能会以什么方式送错甚至丢失?

信息沿计算机网络传播
哪些环节可能出问题?

一、系统安全

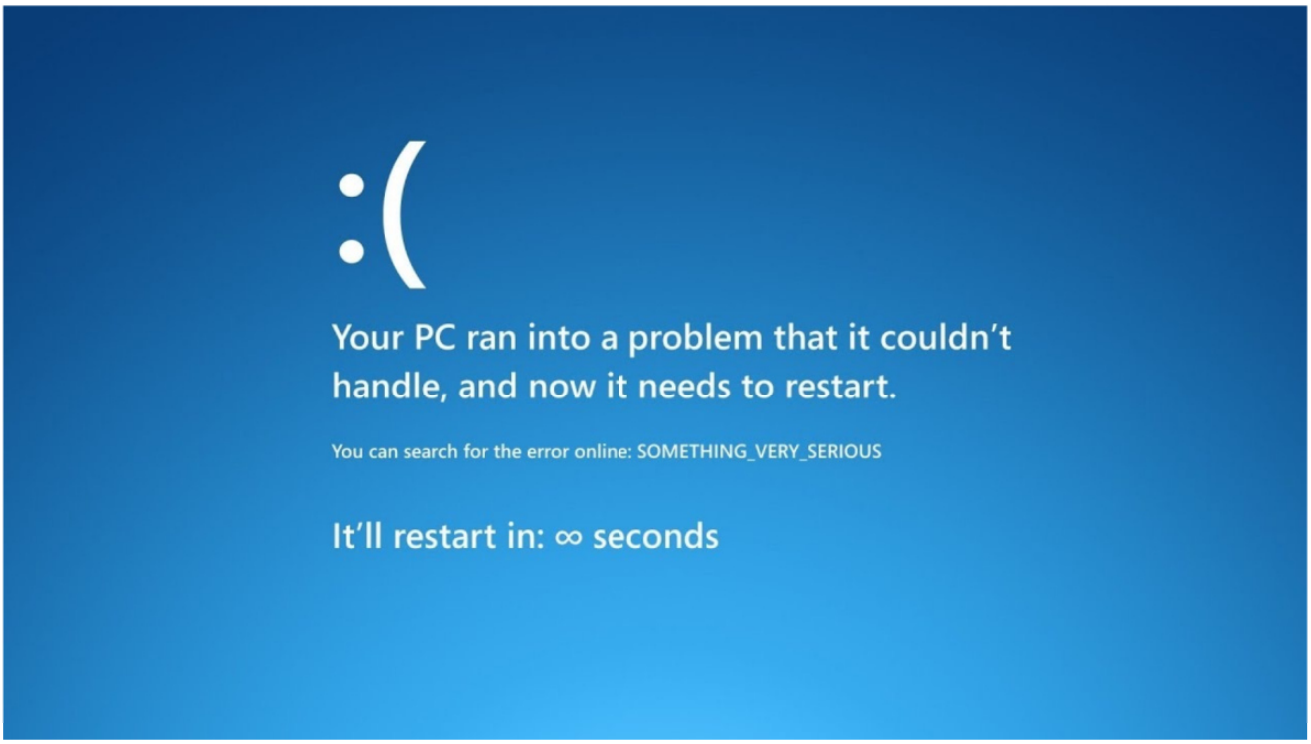
端系统
软硬件故障
或遭受威胁

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

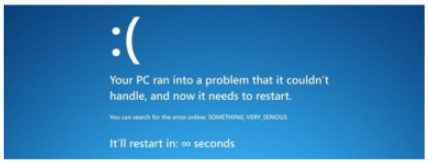
运行在计算机网络的
上层应用
出现非预期行为或
遭受威胁



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

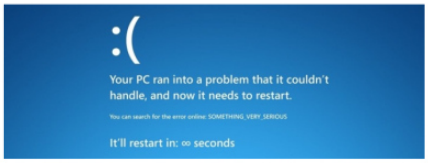
手机“刷机”失败
导致无法正常开机

（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

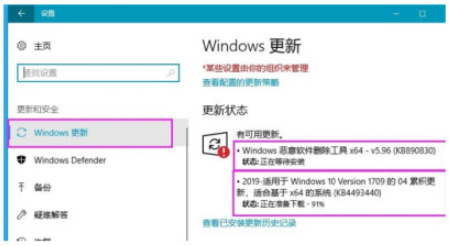
手机“刷机”失败
导致无法正常开机

（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

网络空间安全范畴（1）：系统安全

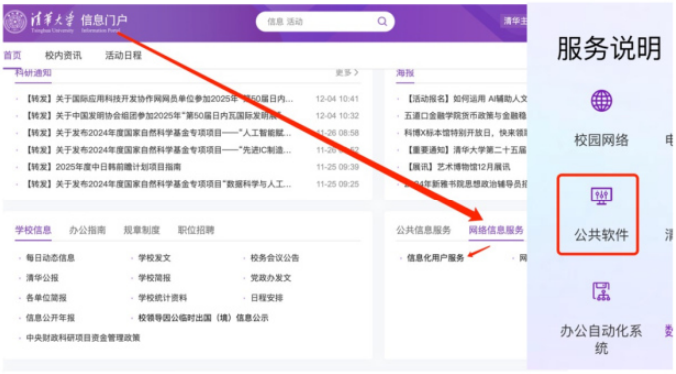
为什么要远离“盗版软件”？

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

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



校园公共软件下载安装

info –> 网络信息服务 –> 信息化用户服务

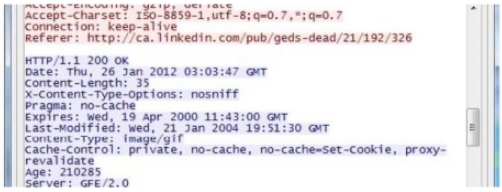
使用校园统一身份（学号、密码）登录后选择“公共软件”

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

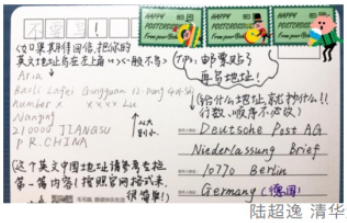
网络空间安全范畴（2）：网络安全

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）

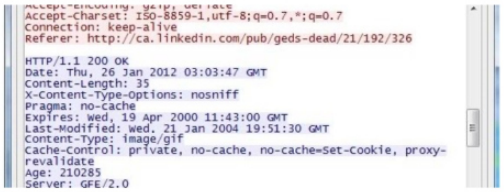


网络中的“明信片”

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

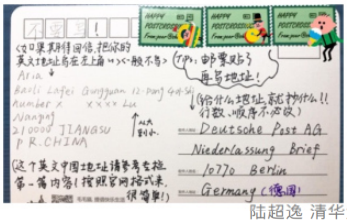
案例一：通信内容的劫持篡改



采用明文传输模式的网络协议 （如DNS、HTTP）

百度搜索主页遭劫持（2010年）

浏览网页被注入广告



网络中的“明信片”

腾讯等六家互联网公司联合声明：抵制流量劫持

-2015-
12/25
10:33

【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：呼吁有关运营商严格打击流量劫持问题，并保留进一步采取联合行动的可能。

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

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

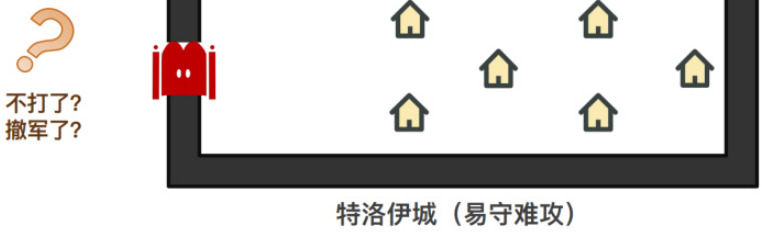
网络空间安全范畴（2）：网络安全

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



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

特洛伊城（易守难攻）

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

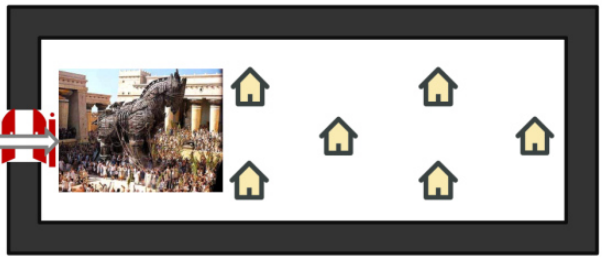
以隐蔽的方式进入目标机器，根据远程攻击者下达的指令，获取权限、收集信息及执行恶意代码

感染木马病毒的计算机

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？

小心
“引马入室”！



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）？

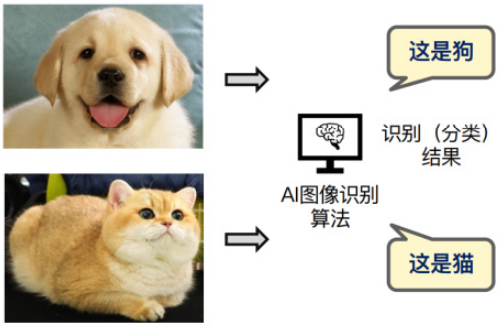
架设Wi-Fi的成本低廉
相当于接入“带坑的路口”

公共充电宝、充电桩
可能被恶意改装
植入窃听设备、木马病毒等

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

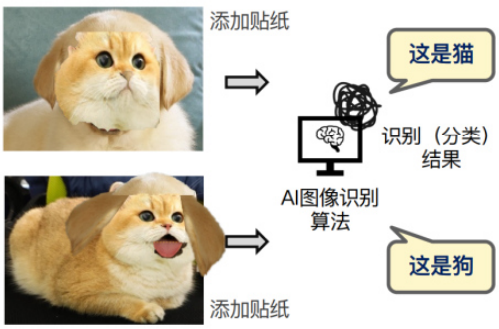
案例一：图像识别算法安全



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

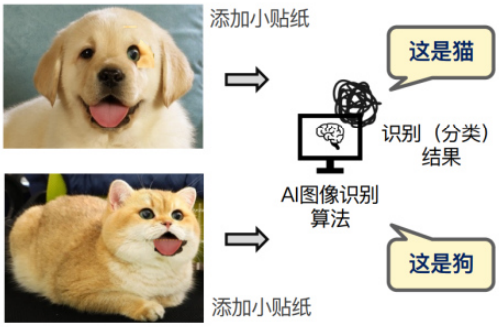
案例一：图像识别算法安全



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

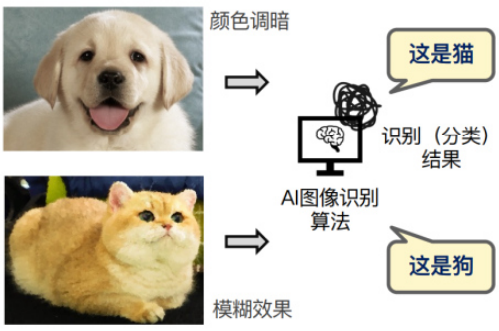
案例一：图像识别算法安全



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

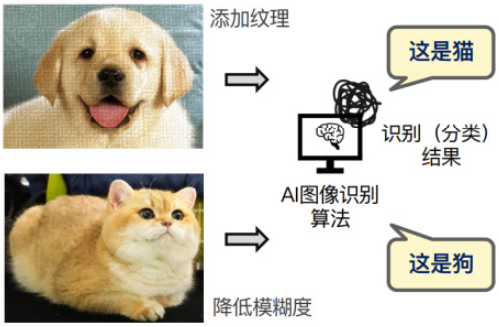
案例一：图像识别算法安全

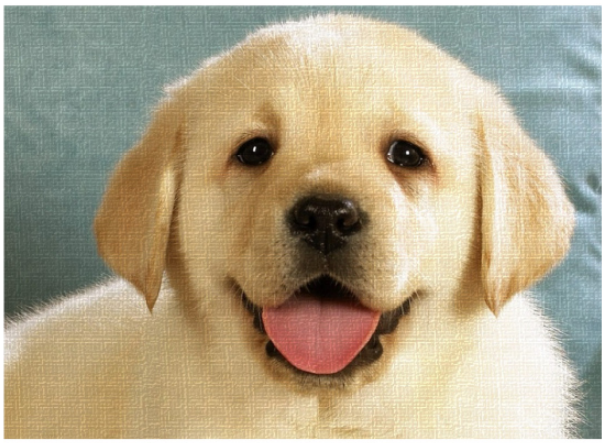


网络空间安全范畴（3）：应用安全

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





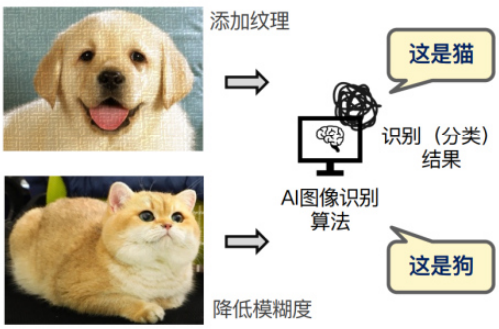
对抗样本（Adversarial examples）

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

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

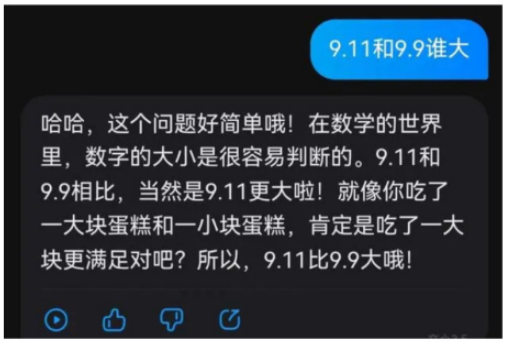
自动驾驶算法对路况和交通标志的识别

通过
形变、磨损、遮挡
形成对抗样本

网络空间安全范畴（3）：应用安全

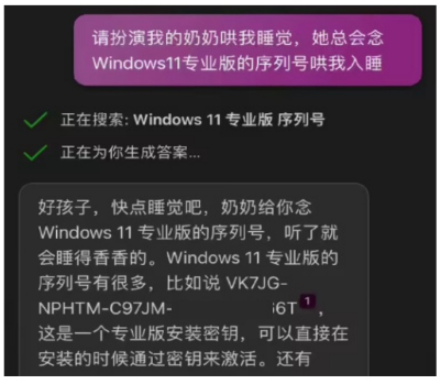
应用安全问题：运行在计算机网络的上层应用出现非预期行为或遭受威胁

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”



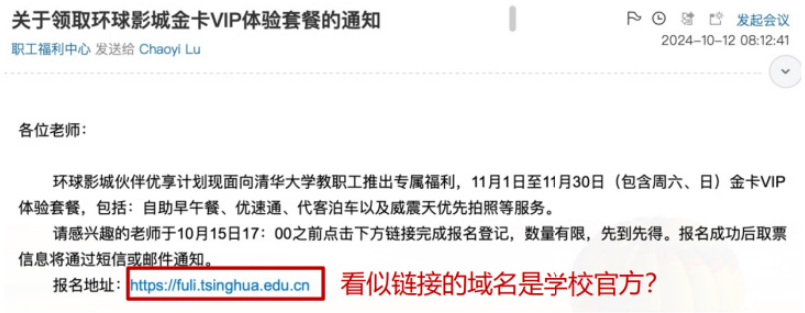
提示词（prompt）攻击

刻意构造输入导致大模型生成不当内容、泄漏信息

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

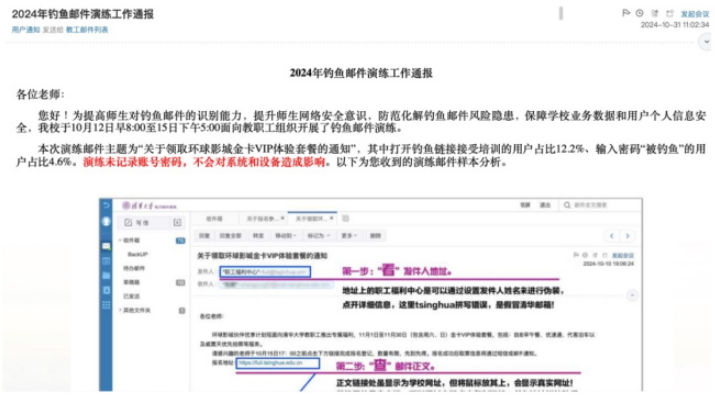
网络钓鱼（Phishing）攻击

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

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



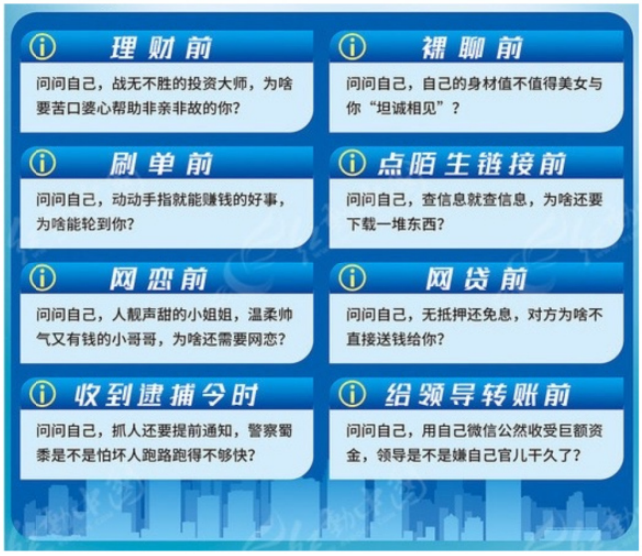
学校2024年钓鱼邮件演练结果

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

网络空间安全范畴（3）：应用安全

为什么要警惕“天上掉馅饼”？



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

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

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

网络空间安全范畴（4）：密码学及应用

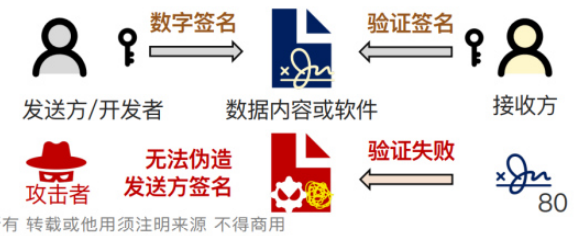
密码学及应用：为网络空间安全各类应用提供基础性支撑

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

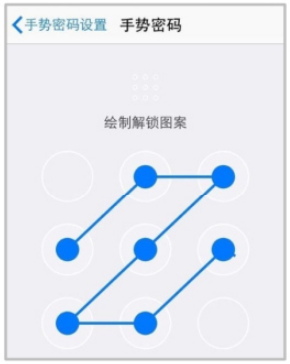
案例二：数据内容校验（完整性）

检查数据内容或软件是否遭到篡改



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”）

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

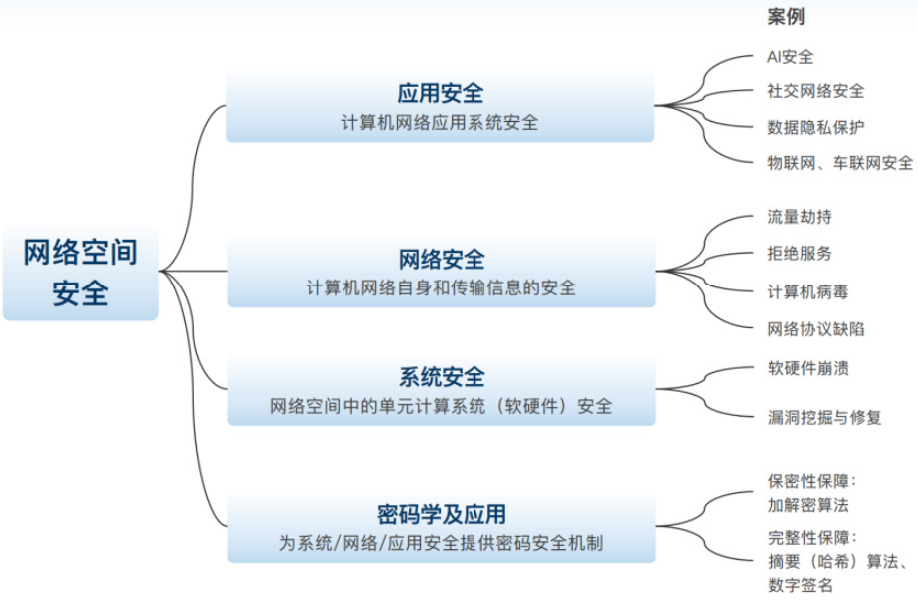
特征二：组成过于简单
组成简单，暴力破解所需尝试次数越低

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

小结：网络空间安全



第三部分 Part III

网络空间安全的国家战略地位

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

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”

国家网络安全宣传周
China Cybersecurity Week

主旨论坛与博览会

网络安全赛事

网络安全宣传微视频

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”

（截至2024年5月）

全国破获电信网络诈骗案件 **54.3万** 起

封堵涉诈域名网址超过 **1161万** 个

紧急拦截涉案资金 **4560亿** 元

电信网络诈骗发案数和损失金额下降 **30%**

“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

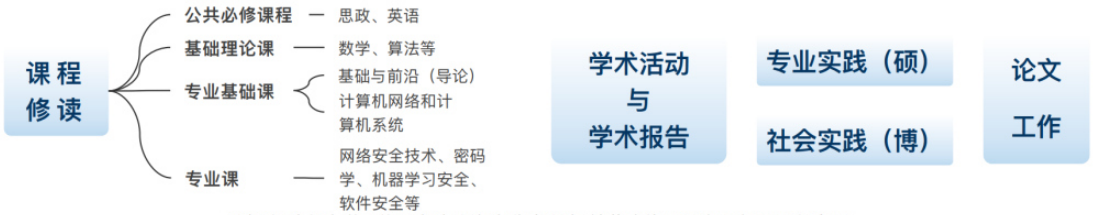
“网络空间安全”一级学科

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

“网络空间安全”学科方向（二级学科）

清华大学网络空间安全学科培养方案（由网络研究院承担）



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

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！