第一章 绪论

周满
15271802577
zhouman@hust.edu.cn
华中科技大学网络空间安全学院

绪论

- 一、安全概念回顾
- 二、多媒体应用的特点
- 三、多媒体数据安全
- 四、实例-云视频监控

信息安全的内涵

- 从最初的信息保密性提升到信息安全保障能力，在发展中逐渐形成一个综合性交叉学科领域

三个重要概念

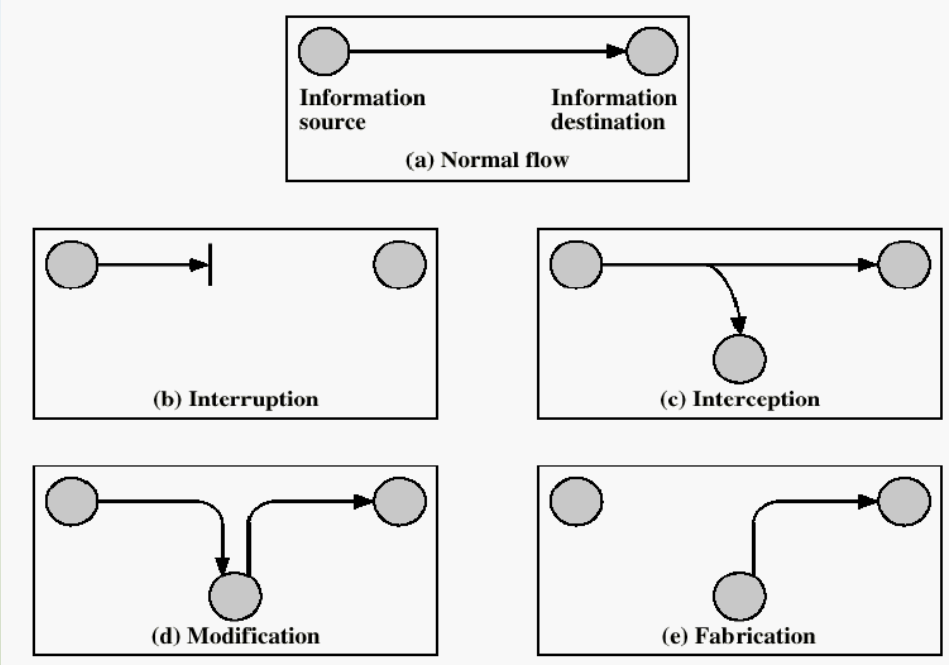
- 需要系统定义**安全需求**
- 三个方面:
  - **安全攻击**
  - **安全服务**
  - **安全机制**

安全攻击

- 任何损害信息安全的行为
  - 信息安全的目的是如何检测、阻止和防御攻击
- 攻击的手段多种多样
  - 包括非授权访问、信息篡改、身份伪装、拒绝服务攻击等等

安全攻击分类

- 被动攻击不影响通信，采用窃听监听通信等手段来:
  - 获取通信内容
  - 监控通讯流量
- 主动攻击会修改数据流来:
  - 伪装身份
  - 重放信息
  - 篡改信息
  - 拒绝服务



安全服务

- 安全服务即增强数据处理系统和信息传输过程安全性的服务
- 信息安全服务的内涵随着信息技术的发展与应用的不断深入也在不断延伸，最开始包括保护信息的机密性、完整性和可用性，但这仅是面向个人用户的信息数据保密
- 后来发展到信息的完整性、可用性、可控性和不可否认性，进而又发展到“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术

安全服务(X.800)

- **认证**-确认实体身份。实体包括：用户、进程、系统、信息等
- **访问控制**- 防止非授权访问
- **数据机密性** - 保护数据非授权泄漏
- **数据完整性**- 确保接收数据和发送数据一致
- **不可抵赖性**-要求无论发送方还是接收方都不能抵赖所进行的传输

Extensions: Availability; Accountability; Reliability; Efficiency; Recoverability et al.

安全机制

- 被设计用于检测阻止安全攻击或者从安全攻击中恢复的机制
- 单一的安全机制是无法满足所有安全服务需求的
- 安全机制的基础是一些基本的安全技术:
  - 加密技术
  - 数字水印
  - ...

利用**安全机制**提供**安全服务**对抗**安全攻击**

小结

- 利用各种基本安全技术构建的安全机制来提供安全服务防护安全攻击
- 如何设计安全机制？
  - 首先针对安全攻击，分析其安全需求
  - 寻找一些现有安全技术构建安全防护机制
  - 如果没有现成的安全技术，需改进或者创新地设计新型安全技术

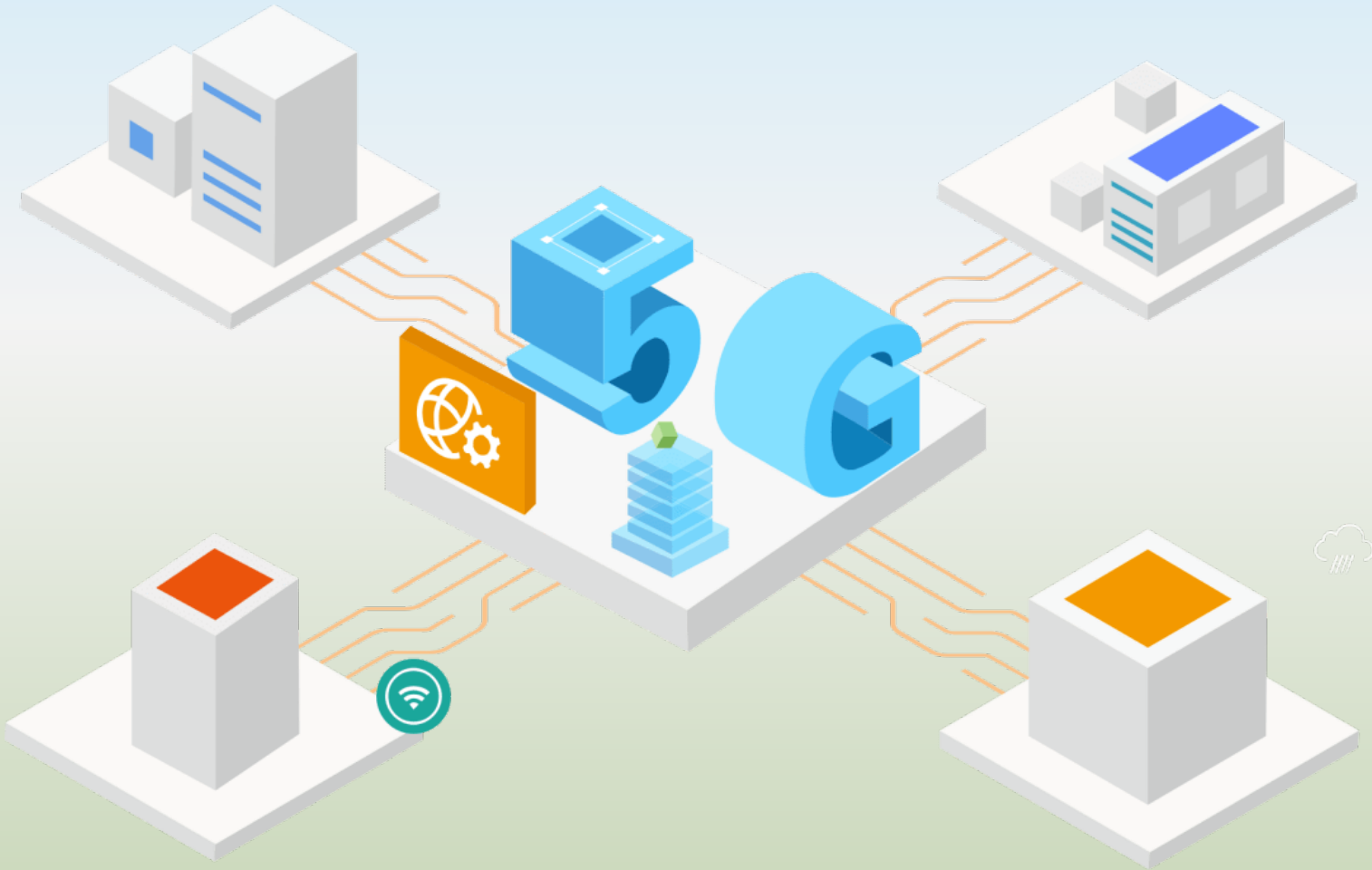
如何实现多媒体大数据的安全保护？

绪论

- 一、安全概念回顾
- 二、多媒体应用的特点
- 三、多媒体数据安全
- 四、实例-云视频监控

多媒体应用的特点

- 数据传输速率高



多媒体应用的特点

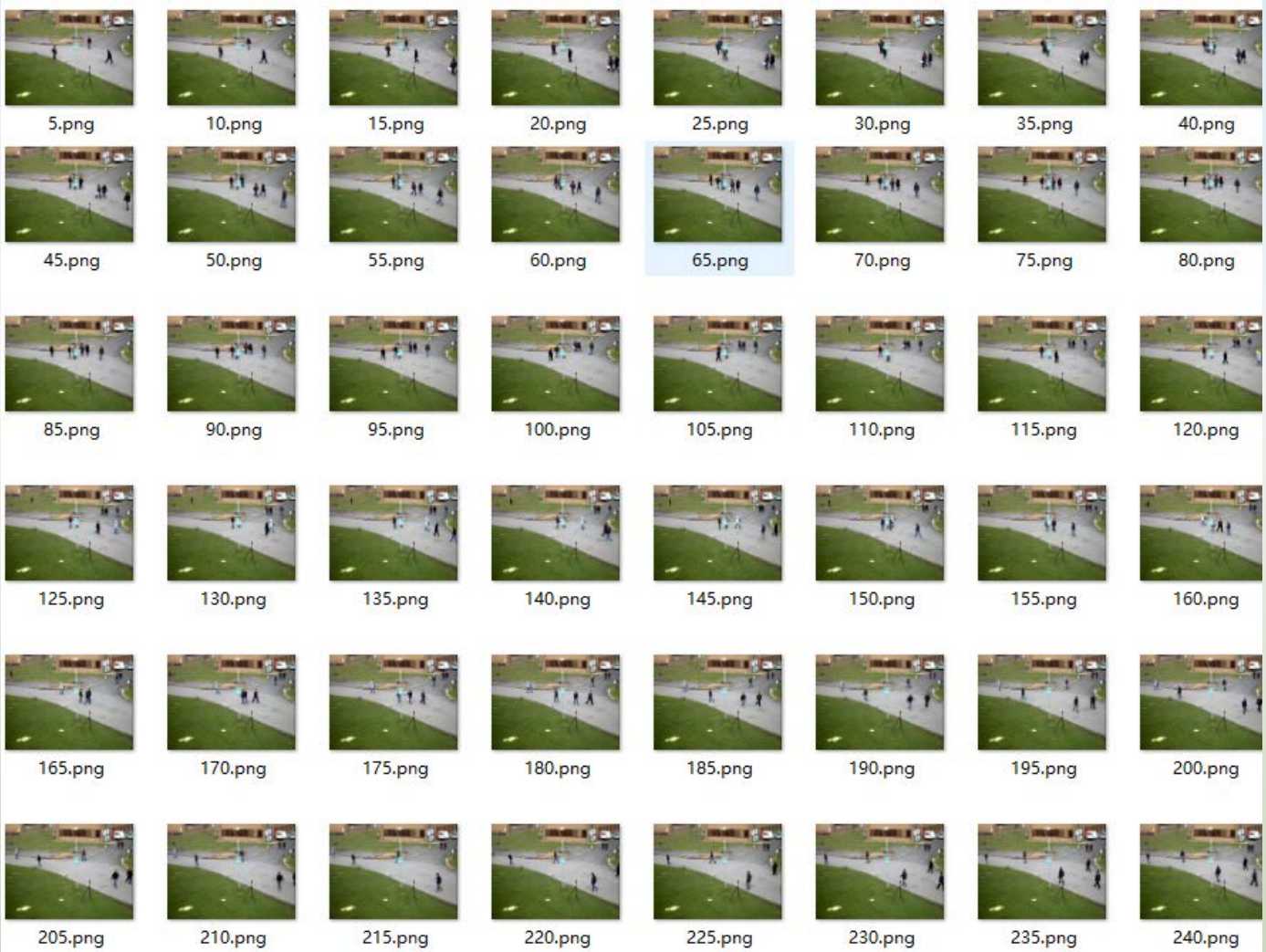
- 耗电量大

多媒体应用的特点

- 受实时约束

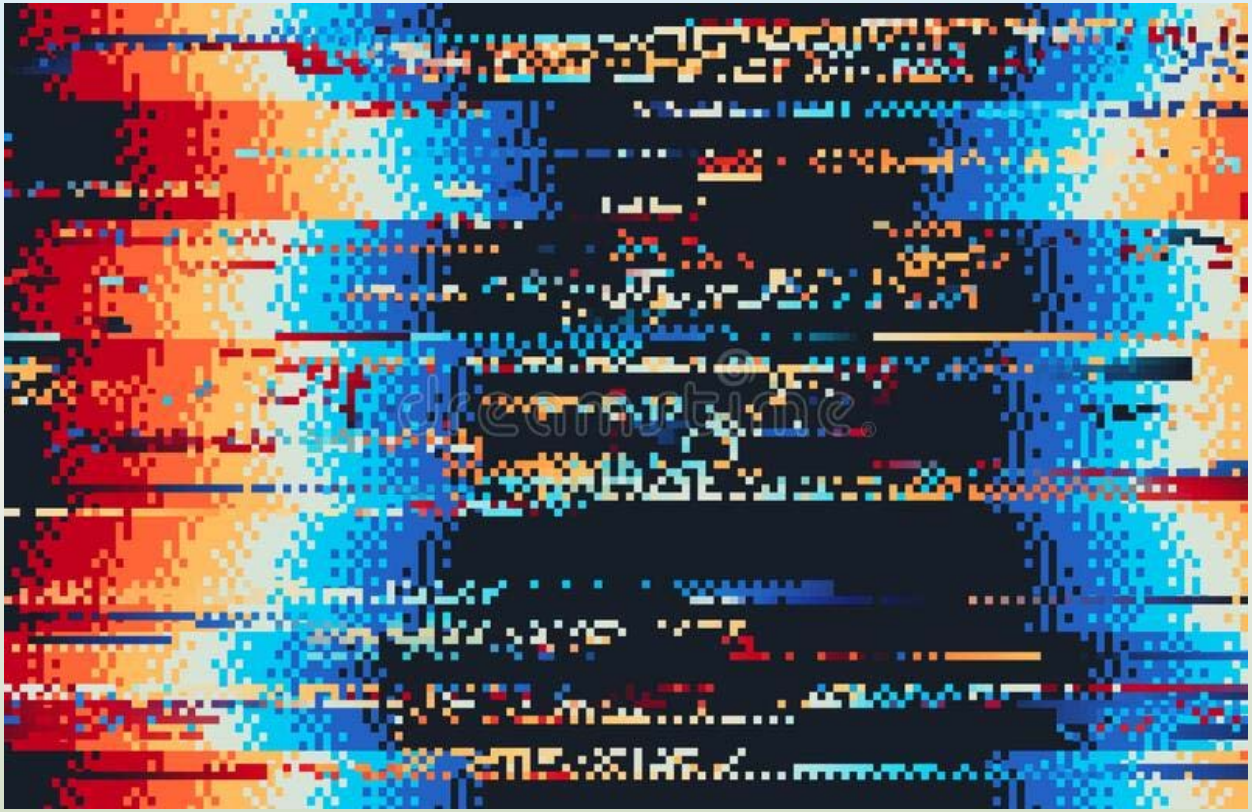
多媒体应用的特点

- 视频画面时间连惯性高



多媒体应用的特点

- 容错率非常低



视频文件小错误引起的画面瑕疵

多媒体应用的特点

- 内容价值差别大

多媒体应用的特点

- 多层次语义内容

多媒体应用的特点

- 传输渠道及形式多样化

报纸

广播

DVD

卫星电视

无线网络

智能手机

绪论

- 一、安全概念回顾
- 二、多媒体应用的特点
- 三、多媒体数据安全
- 四、实例-云视频监控

对多媒体数据的攻击

- 对可用性的攻击：
  - 系统的多媒体被破坏或变得不可利用，不能使用
  - 如在通信中多媒体的损坏、不能解码或失去观赏功能
- 对保密性的攻击：
  - 未授权方通过截获等手段非法获取信息并对某多媒体信息非法访问
  - 如在网络上搭线窃听以获取数据，违法复制文件或程序

对多媒体数据的攻击

- 对完整性的攻击：
  - 未授权方破坏多媒体信息资产，改变多媒体数据文件中的数据，篡改在网络中传输的多媒体信息内容，采用软件修改多媒体内容
- 对真实性的攻击：
  - 未授权方伪造和替换原有的多媒体信息，对多媒体的来源进行伪造，例如在数字图像中伪造水印信息

多媒体数据的安全服务

- 保障多媒体数据的源头安全
  - 在数字产品产生时嵌入数字水印以便保护版权；对需要保密的信息加密处理防止非授权访问和获取；利用生物特征识别用户
- 保障多媒体数据的传输安全
  - 加密后传输密文；利用信息隐藏传递秘密信息；生物特征加密或变形以防止生物模板泄漏

多媒体数据的安全服务

- 保护多媒体数据获取的安全
  - 数字媒体中嵌入数字指纹用于追踪数字产品分发和用户的权益，感知哈希对获取信息进行验证以保障获取信息的可信性
- 多媒体数据的真实性鉴别
  - 向数字产品中加入数字水印来鉴别和认证来源
  - 利用数字媒体取证技术对多媒体作品进行盲检测，鉴别数据来源、判断篡改与否

性能需求

- 多媒体数据比特率高，通常以压缩格式传输和存储
  - 安全保护机制需要与不同的压缩标准兼容，而且不影响压缩效率
- 多媒体内容分析需要复杂算法
  - 安全保护机制需要支持复杂保护算法，而且不能影响多媒体应用的功能
- 多媒体数据为用户服务
  - 安全保护机制需要对用户透明，尽量避免对用户体验造成影响

性能需求

- 多媒体内容常包括大量不同部分，各部分具备不同程度的敏感性
  - 现有基于文件的安全保护模型不再适用，多媒体安全保护机制需灵活支持不同级别的访问控制
- 多媒体数据应用通常使用大量实时数据来保证高质量服务，效率至关重要
  - 安全机制需要实时处理快速到达的大量数据
- 多媒体数据网络传输有特殊需求
  - 安全机制需考虑网络友好性，考虑加密、信号处理和网络技术的互操作性；降低对现有和未来网络技术的影响

安全保护机制

- 信息隐藏
- 数字水印
- 身份认证
- 多媒体加密
- 多媒体数据隐私保护
- 多媒体取证
  - 多媒体篡改定位
  - Deepfake检测
- 多媒体数据对抗防御
- 多媒体数据内容恢复
- 安全转码

绪论

- 一、安全概念回顾
- 二、多媒体应用的特点
- 三、多媒体数据安全
- 四、实例-云视频监控

视频监控

- 视频监控系统被广泛应用在公共场合

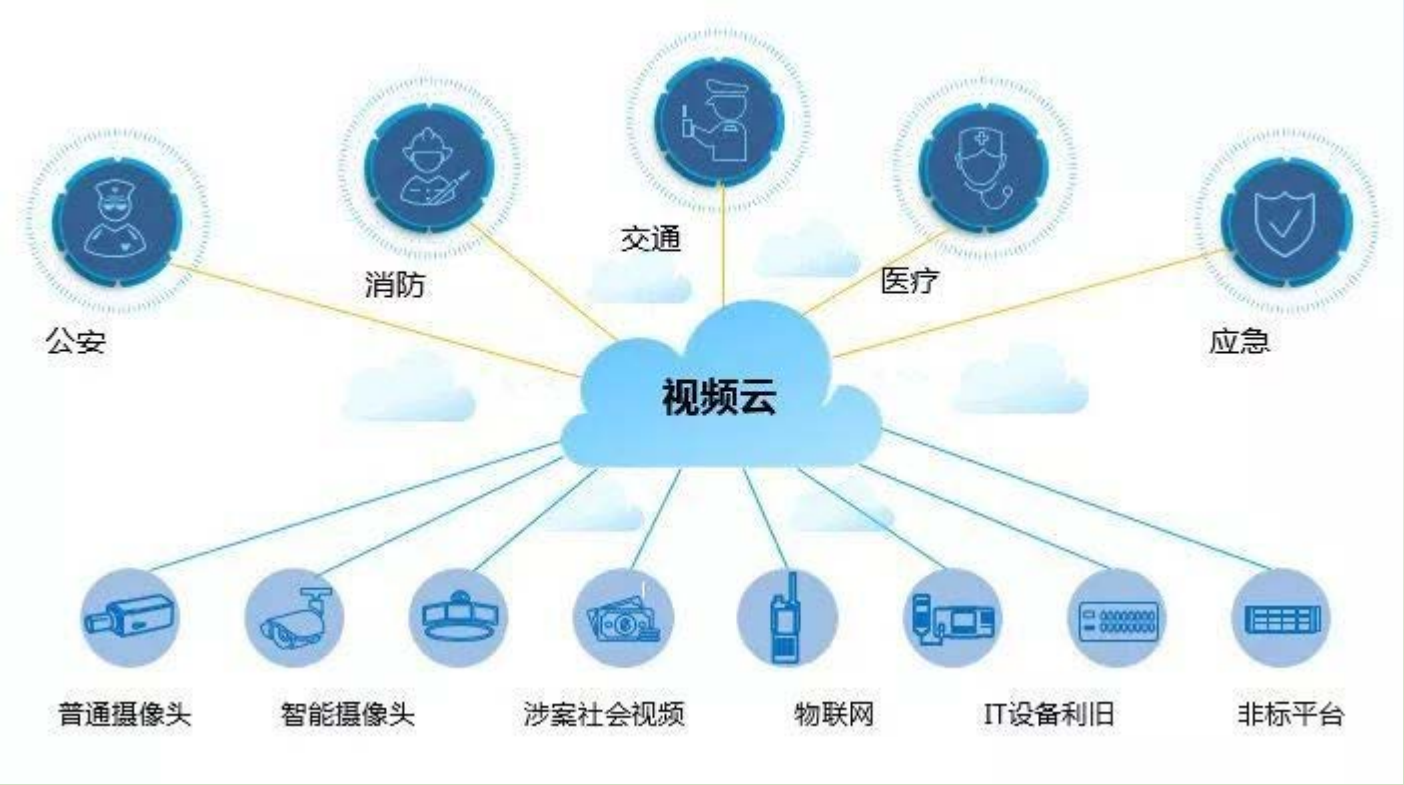
视频监控

- 视频监控系统被广泛应用在公共场合

例如在2013年的波士顿马拉松爆炸事件调查中，为确认恐怖分子的身份发挥了关键作用

云视频监控

- 一个快速发展的领域
- 优点：灵活性



云视频监控

- 一个快速发展的领域
- 优点：泛在性

云视频监控

- 一个快速发展的领域
- 优点：健壮性

HIKVISION
海康威视

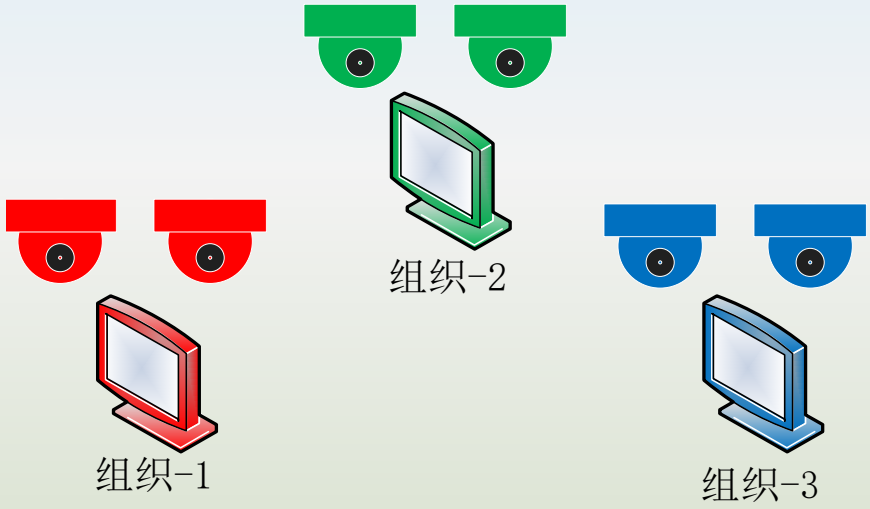
云存储服务

- 动态视频与图片自动备份到云端，随时随地想看就看
- 不限容量安全存储最近7天的视频与图片，1年期限全免费
- 全面支持C1、C2设备，多样的选择，一样的服务

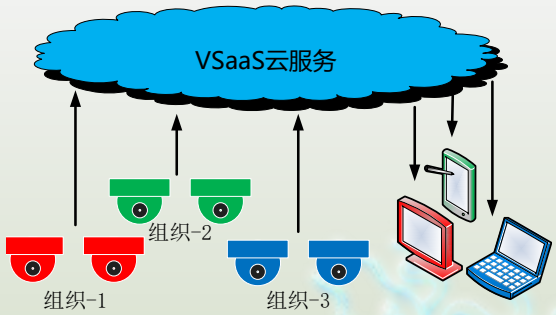
萤石
EZVIZ

讨论：安全威胁

- 云视频监控对安全性提出更高要求。
- 问题：云端能够解密用户的监控视频内容



传统视频监控系统：
1. 各组织（机构/家庭）自行搭建视频监控系统；
2. 封闭式管理；
3. 单个恶意或被攻破组织不会影响其它；



云视频监控系统：
1. 各组织（机构/家庭/个人）安装监控摄像头；
2. 租用云平台管理、存取与智能报警；
3. 恶意或被攻破的云平台将泄露所有的监控视频数据；

讨论：需求分析

- 功能：
  - 内容/事件检测
- 安全性：
  - 加密保护
  - 访问控制
- 完整性：
  - 身份认证
  - 多媒体取证
- 效率：
  - 提高准确率
  - 降低存储量
  - 减少传输时间

讨论：安全机制

- 加密
- 认证
- 数字水印
- 隐私计算