电子数据取证技术趋势研究

王丽波

2016-7-8

01 电子数据取证的现状

电子数据证据概述

第四十八条 可以用于证明案件事实的材料，都是证据。

证据包括：

（一）物证；

（二）书证；

（三）证人证言；

（四）被害人陈述；

（五）犯罪嫌疑人、被告人供述和辩解；

（六）鉴定意见；

（七）勘验、检查、辨认、侦查实验等笔录；

（八）视听资料、电子数据。

证据必须经过查证属实，才能作为定案的根据。

电子数据取证行业标准

GB/T 29360-2012 电子物证数据恢复检验规程	GA/T 978-2012 网络游戏私服检验技术方法
GB/T 29361-2012 电子物证文件一致性检验规程	GA/T 1069-2013法庭科学电子物证手机检验技术规范
GB/T 29362-2012 电子物证数据搜索检验规程	GA/T 1070-2013法庭科学计算机开关机时间检验技术规范
GA/T 754-2008 电子数据存储介质复制工具要求及检测方法	GA/T 1071-2013法庭科学电子物证Windows操作系统日志检验技术规范
GA/T 755-2008 电子数据存储介质写保护设备检测方法	GA/T 1770-2014 《移动终端取证检验方法》
GA/T 756-2008 数字化设备证据数据发现提取固定方法	GA/T 1771-2014 《芯片相似性比对检验方法》
GA/T 757-2008 程序功能检验方法	GA/T 1772-2014 《电子邮件检验技术方法》
GA/T 825-2009 电子物证数据搜索检验技术规范	GA/T 1773-2014 《即时通讯记录检验技术方法》
GA/T 826-2009 电子物证数据恢复检验技术规范	GA/T 1774-2014 《电子证据数据现场获取通用方法》
GA/T 827-2009 电子物证文件一致性检验技术规范	GA/T 1775-2014 《软件相似性检验技术方法》
GA/T 828-2009 电子物证软件功能检验技术规范	GA/T 1776-2014 《网页浏览器历史数据检验技术方法》
GA/T 829-2009 电子物证软件一致性检验技术规范	《计算机犯罪现场勘验与电子证据检查规则》（公信安〔2005〕161号）
GA/T 976-2012 电子数据法庭科学鉴定通用方法	《公安机关电子数据鉴定规则》（公信安〔2005〕281号）
GA/T 977-2012 取证与鉴定文书电子签名	

现场取证与网络取证

现场取证	网络取证
静态取证	动态取证
事后取证	事中取证
证据链的发端	证据链的构成
软硬件的恢复技术	数据抓取技术
数据格式分析与检索技术	海量数据与协议分析技术

网络取证的内容

- 来源取证：确定犯罪嫌疑人和它所在位置

  取证内容主要包括IP地址、MAC地址、电子邮件、软件帐号等。

- 事实取证：确定犯罪实施的具体内容和过程

  取证内容主要包括网络状态和数据包的分析、日志文件分析、文件内容调查、使用痕迹调查、软件功能分析、软件相似性分析等。

网络取证相关技术

- 网络数据包分析取证技术
- IDS、防火墙、VPN取证技术
- 蜜阱取证技术
- 隐蔽代码取证技术
- 数据挖掘技术

通用网络数据包分析取证工具

工具名称	使用环境	特性
TcpDump&Windump	Unix & Windows	采集过滤
Wireshark	Unix & Windows	采集过滤
Sleuth Kit	Unix	采集过滤、流重组、数据关联
Argus	Unix	采集过滤、日志分析
SNORT	Windows /Unix	采集过滤

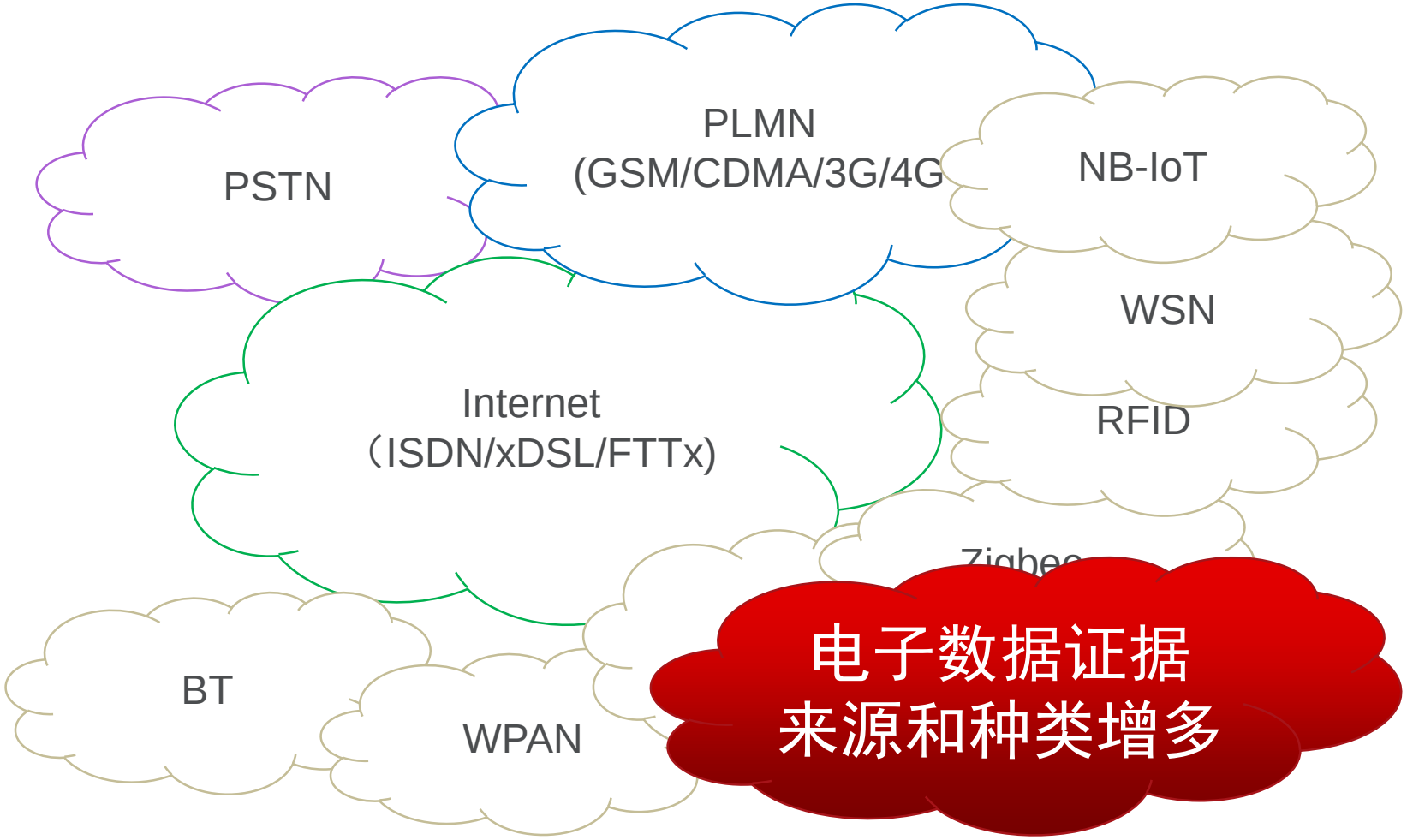
电子数据取证的挑战

泛在网络

云计算

人工智能

泛在网络(UbiquitousNetwork)



02

物联网取证趋势

互联的时代

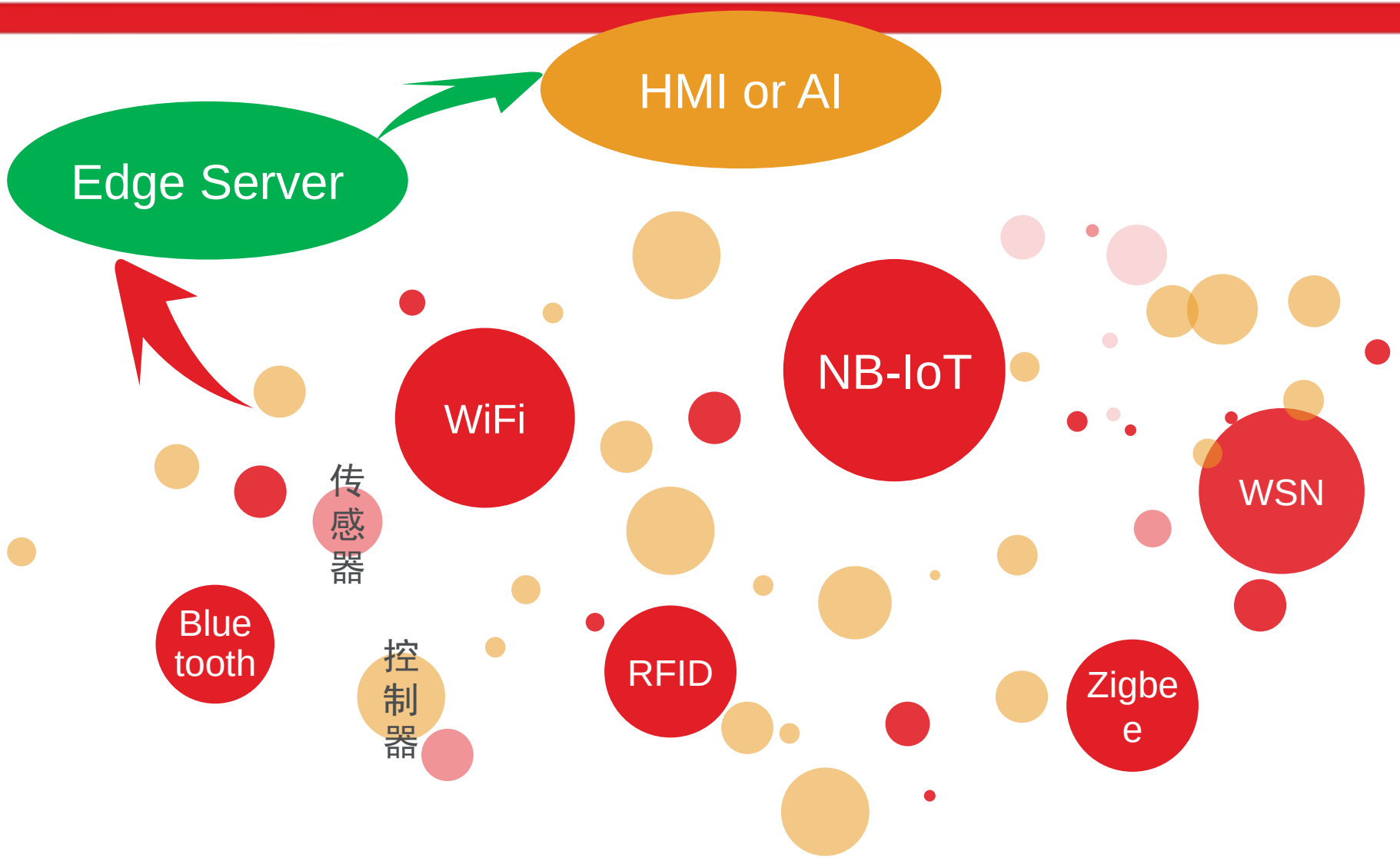
- 互联网

  人人互联（H2H）

- 物联网(Internet of Things，IoT)

  人物互联（H2M）、物物互联（M2M）、虚拟/现实互联（V2R）

物联网架构


HMI or AI
Edge Server
WiFi
NB-IoT
WSN
传感器
Blue tooth
控制器
RFID
Zigbee

物联网环境下的安全风险

01

物理安全

物理俘获、固件/器件篡改

02

接入层安全

寻址安全、双向认证、动态加密

03

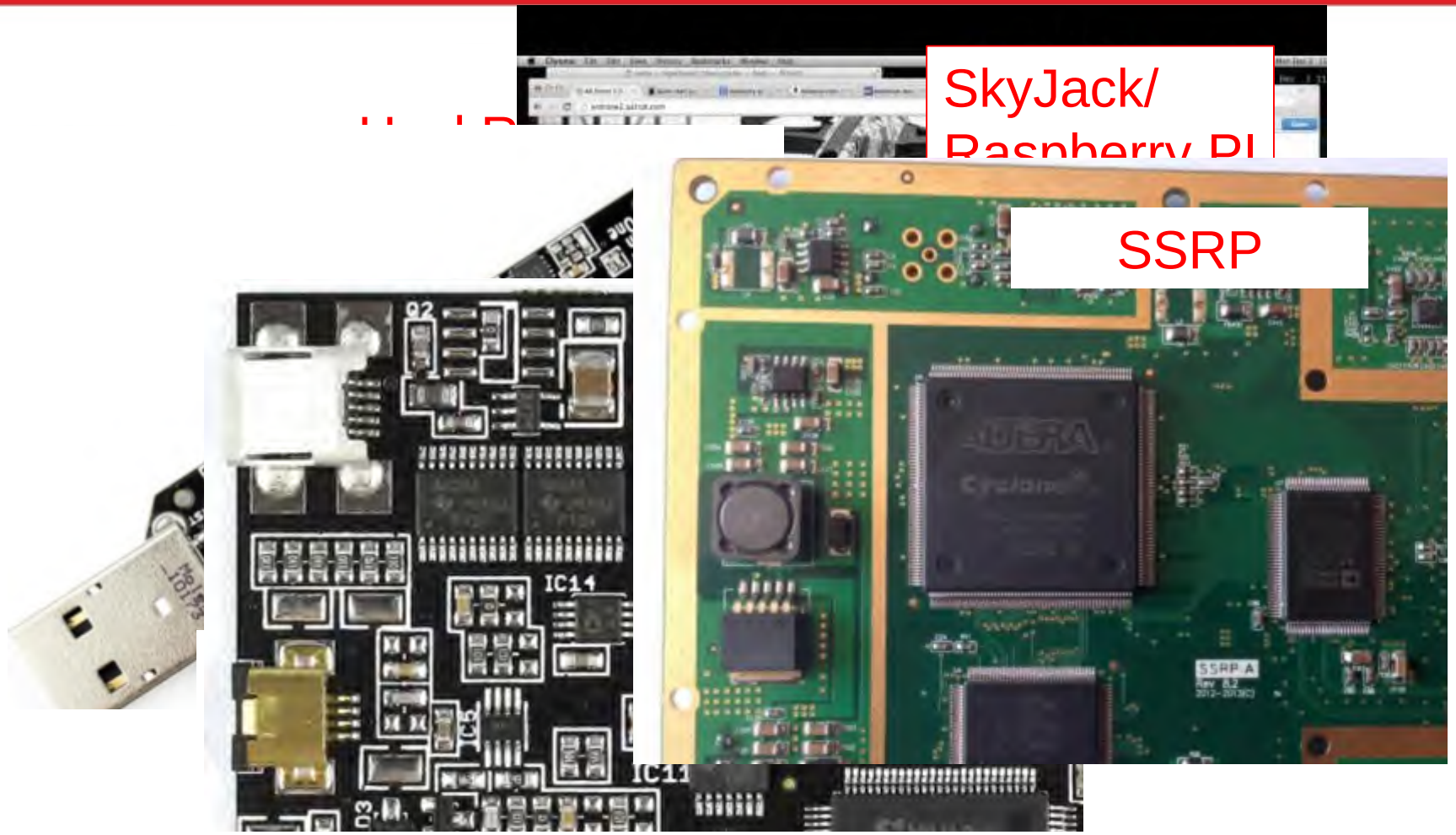
网络层安全

04

应用层安全

数据安全、隐私保护

物联网接入入侵威胁



物联网黑客攻击事件

- 2007年，美国副总统迪克•切尼心脏病发作，疑似心脏除颤器无线连接功能被利用。
- 2008年，土耳其石油管道压力阀控制器被黑客通过联网的监控摄像头漏洞侵入，增大压力引起管道爆炸。
- 2008年，波兰少年改装电视遥控器控制有轨电车系统,导致数列电车脱轨、人员受伤。
- 2011年，伊朗俘获美国RQ-170
- 2013年，美国黑客萨米•卡
- 2014年，特斯拉Tesla Mode
- 2015年，比亚迪云服务漏洞被用于远程控制
- 2015年，切诺基吉普车的联网娱乐系统被入侵，车辆被控制。

从接入层到网络层：
隐患增多、危害更直接

物联网怎能不上“锁”？

物联网取证相关技术：

- 物联网节点“黑匣子”技术
- 物联网分布式IDS技术
- 物联网嗅探取证技术

物联网节点“黑匣子”技术

访问日志

无线入侵检测（分布式IDS）

固件更新日志

操作日志

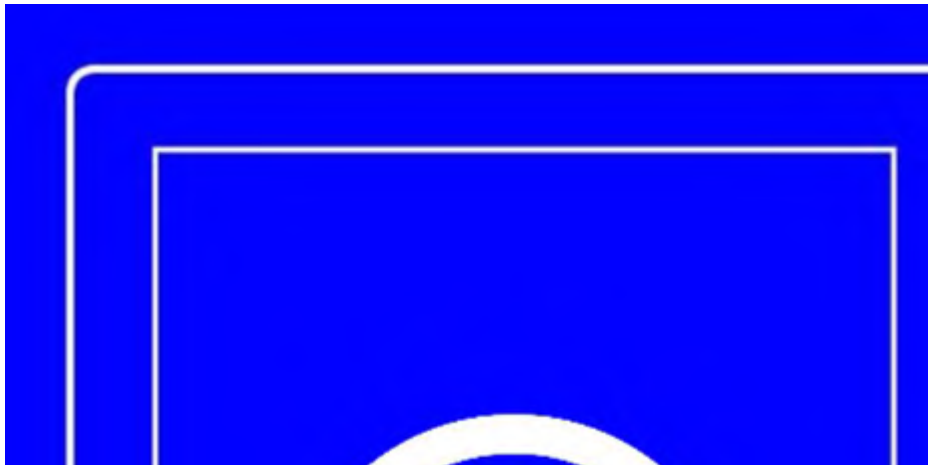
物物关系类型

物联网嗅探取证技术

When？

Where？

Who？



03 云取证趋势

两个不同的概念

云计算环境下的安全风险

cloud security alliance

利用云攻击

破密、DDOS、
垃圾邮件、僵尸
网络控制器

云服务接口

API的安全测试、
渗透测试

契约精神

云服务商滥用权
力访问客户的数
据及应用

资源共享的风险

虚拟化软件出现
漏洞

数据保护意识

不正确的访问控
制或弱加密

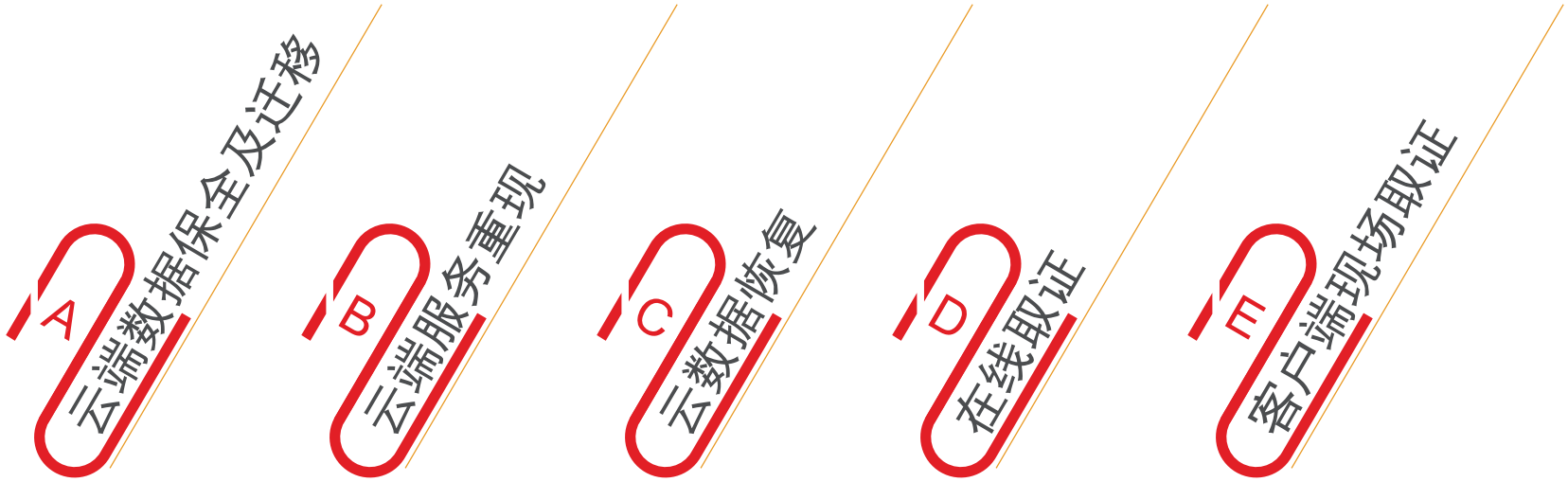
账号或服务劫持

攻击者窃取账户
信息和服务，就
能截获和重定向
客户和云的流量

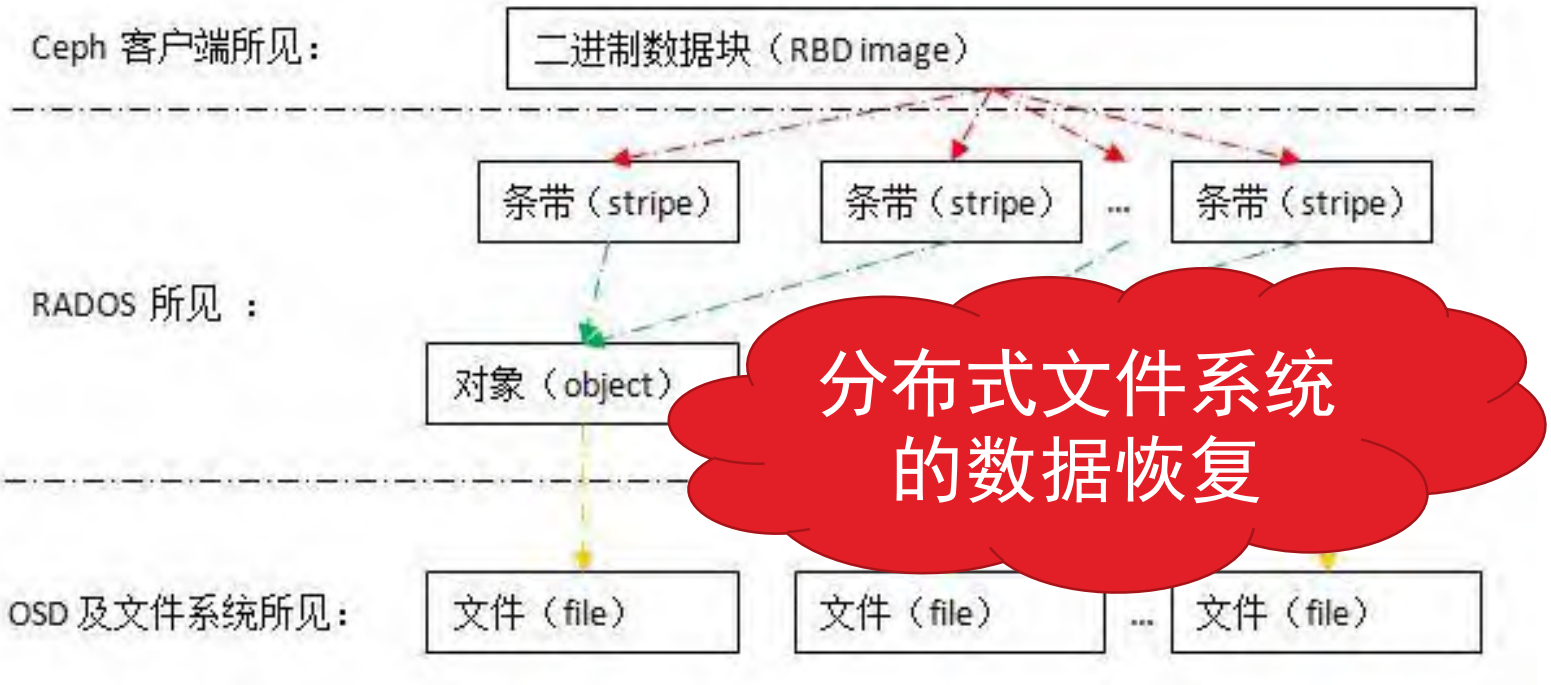
未知风险

云服务商与客户
的信息不对称

云取证相关技术



示例：Ceph存储架构


Ceph 客户端所见：
二进制数据块（RBD image）
条带（stripe）
条带（stripe）
...
条带（stripe）
RADOS 所见 ：
对象（object）
分布式文件系统
的数据恢复
OSD 及文件系统所见：
文件（file）
文件（file）
...
文件（file）

示例：Ceph操作

- 查看vm pool中的文件

  # rbd ls vms

- 查看volume pool中的文件

  # rbd ls volumes

- 导出vm

  # rbd export -p vms <vm的uuid> <导出文件名>

- 导出volume

  # rbd export -p volumes <volume的uuid> <导出文件名>

```
[root@localhost ~]# ll -h
总用量 151G
-rw-------. 1 root root 1.4K Mar  2 11:15 anaconda-ks.cfg
-rw-r--r--  1 qemu qemu 100G Jul 11 13:39 d89a350d-6386-48ef-a92a-4a34f11ec295_disk.img
-rw-r--r--  1 qemu qemu  50G Jul 11 13:22 volume-cb2850ee-d8f8-4696-a806-25d1e8ae3d94
```

示例：virt-manager加载VM


Thanks