物联网安全
Internet of Things Security

第二章：物联网安全概述

冀晓宇
浙江大学

2 物联网安全概述

- 2.1 物联网安全现状
- 2.2 物联网安全威胁
- 2.3 物联网安全特点

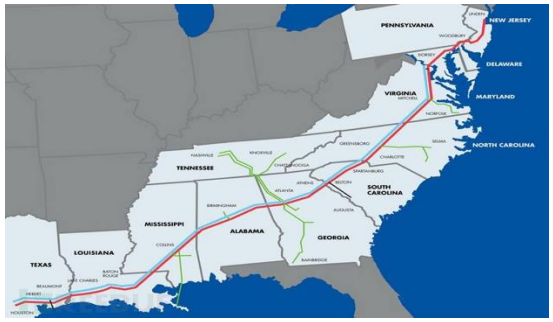
第一节

物联网安全现状

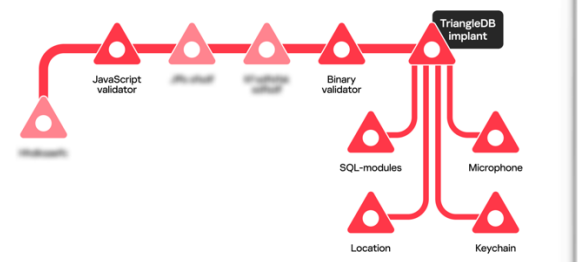
近些年物联网安全事件

2023年10月波音遭受LockBit3.0**勒索软件攻击**

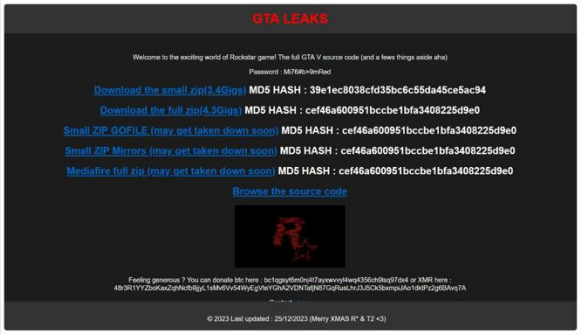
2023年8月福特汽车被曝WiFi驱动存在**缓冲区溢出漏洞**



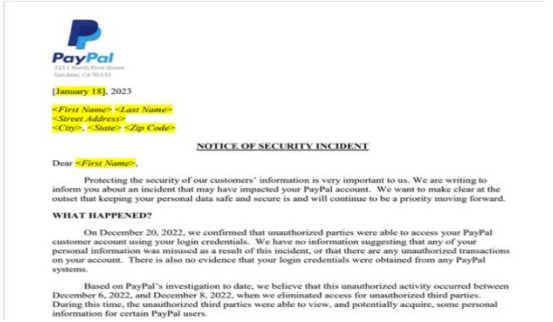
2021年美国一管道公司遭**勒索软件攻击**导致**燃油管道被切断**



2023年披露的三角测量攻击导致大量**iPhone被窃听**



2022年9月Rockstar服务器遭黑客入侵导致GTA5**源码泄露**

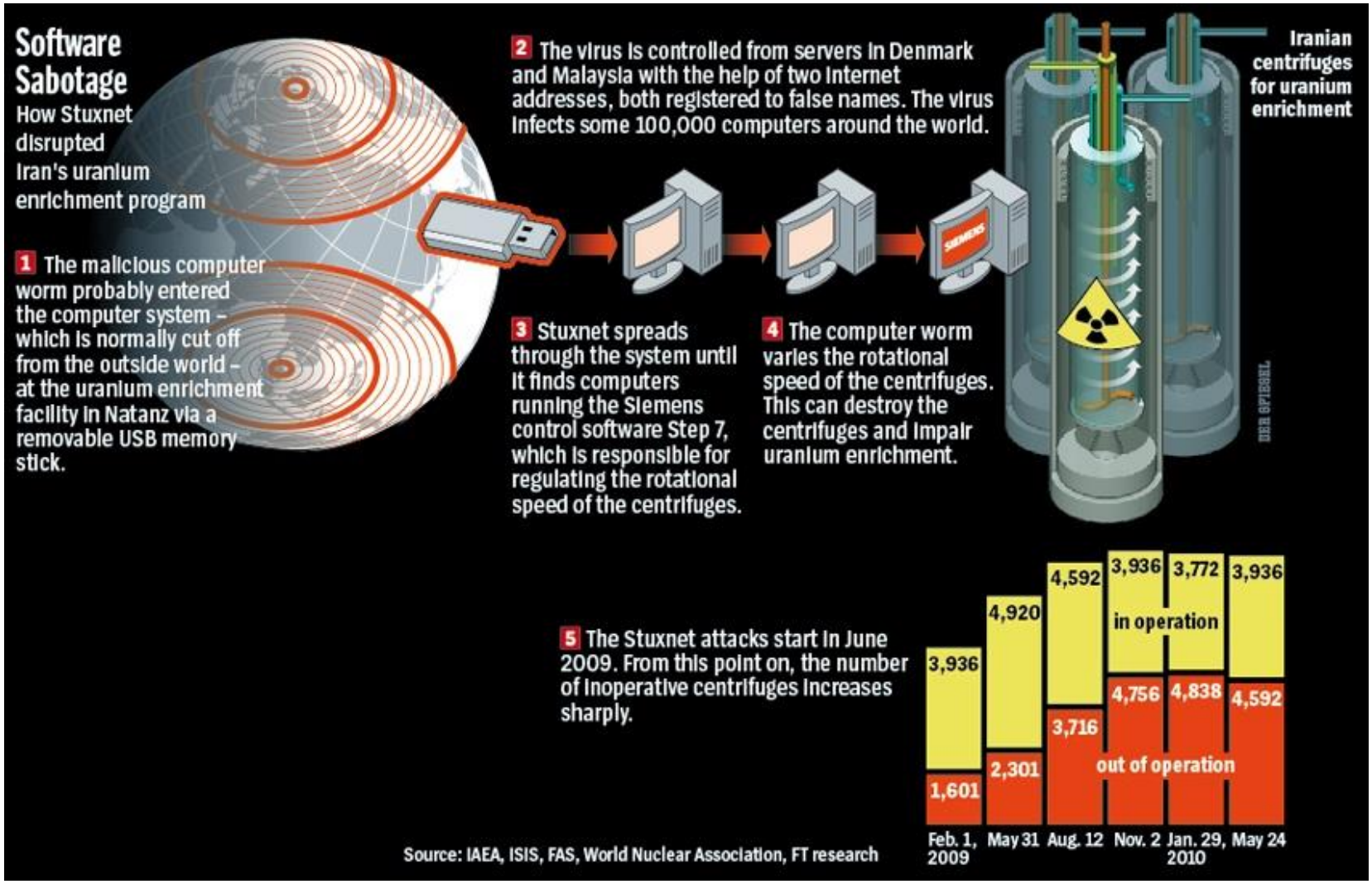


2022年12月PayPal遭**撞库攻击**导致近3.5万**用户资料泄露**

物联网安全：从“谋财”到“害命”

- **“震网”病毒**
  - 2009年6月，定向攻击基础能源设施，包括核电站、国家电网等。攻击控制铀浓缩离心机的可编程控制器（PLC），篡改离心机的运行转速，最终导致大量离心机因超出安全临界速度而毁坏。
  - 它是**首个针对工业控制系统的蠕虫病毒**，复杂性非常罕见，病毒编写者需要对工业生产过程和工业基础设施十分了解。
  - 后果：伊朗核计划滞后两年
- **“害命”**
  - 通过攻击物联网危害到物理世界的实体设备，进而威胁到个人生命安全甚至是国家安全

- **攻击过程**：利用西门子公司控制系统（SIMATIC WinCC/Step7）存在的漏洞，感染数据采集与监控系统（SCADA），向可编程逻辑控制器（PLC）写入代码并将代码隐藏。

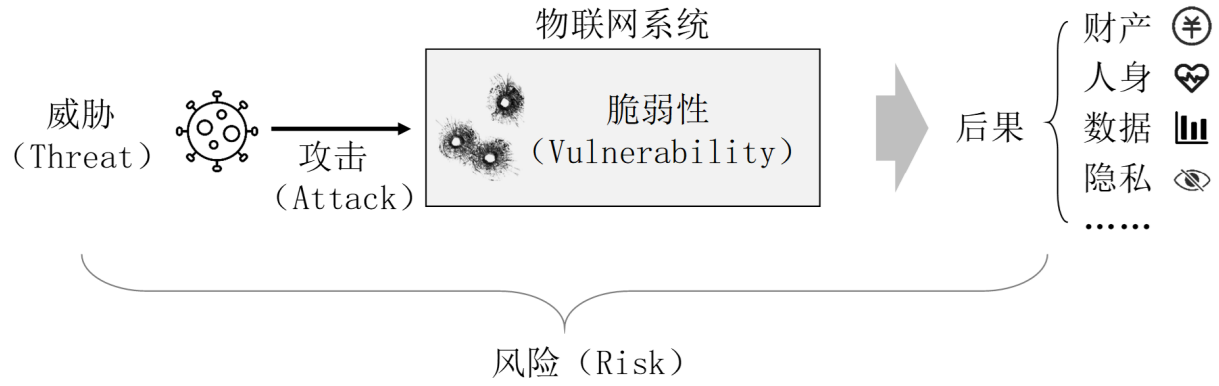



www.President.ir

物联网安全基本概念

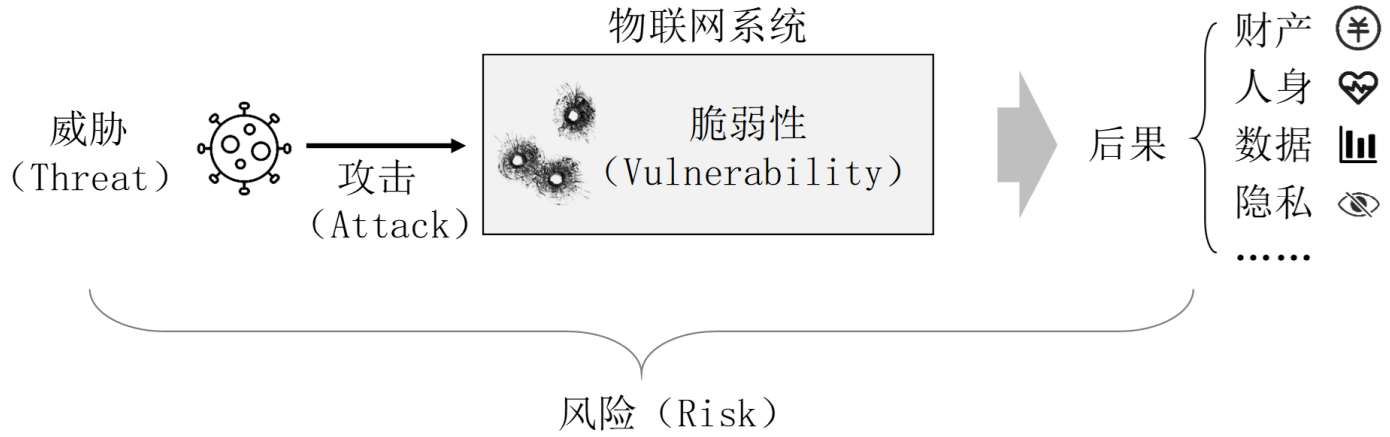
安全名词	内涵
威胁 (Threat)	存在于环境、能力、行动或事件中可能会破坏安全并造成伤害的安全隐患，也就是说，威胁可能利用脆弱性并造成损失。比如勒索软件、蠕虫等恶意程序为有意威胁，地震、洪涝灾害为自然威胁，误操作为无意威胁等。
攻击 (Attack)	蓄意试图规避目标系统的安全服务并违反其安全策略的智能行为。以震网病毒事件为例，通过震网病毒利用PLC脆弱性的行为就是攻击。
脆弱性 (Vulnerability)	系统在设计、实现、操作或管理中的缺陷或弱点，可被攻击者利用以至于给系统造成损失或危害。比如软硬件漏洞，访问权限设置缺陷等。
风险 (Risk)	一种损失预期，表示为某一特定威胁利用某一特定脆弱性产生特定有害结果的可能。

安全概念示意图



物联网安全基本概念

安全概念示意图



- 以震网病毒事件为例：
  - **威胁**：震网病毒（蠕虫病毒）
  - **脆弱性**：U盘管理缺陷、控制系统软件软件缺陷
  - **攻击**：震网病毒利用软件系统如PLC等缺陷的智能行为
  - **风险**：震网病毒作用于PLC之后造成铀浓缩离心机受损的可能

物联网安全 – 定义

- **本课程采用的定义**

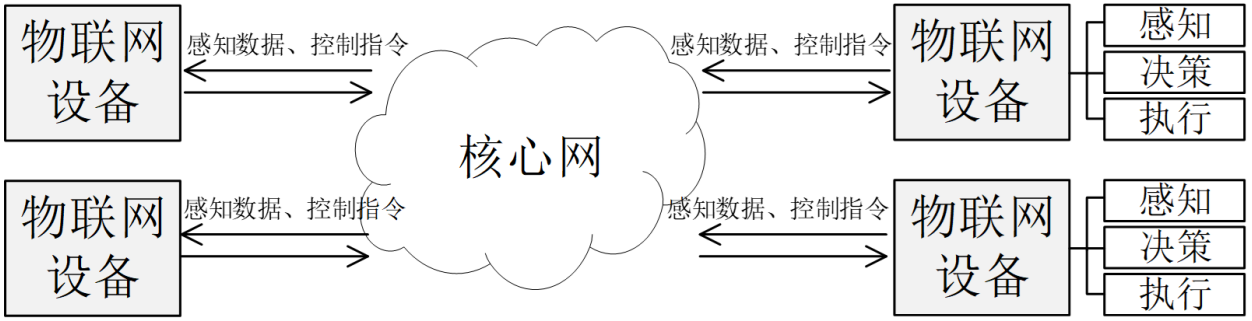
物联网安全就是研究如何分析、检测物联网自身的脆弱性、面临的安全风险和攻击，并在特定业务场景下保护物联网的**感知、计算、传输、控制**等环节的安全。

- 例如，在自动驾驶汽车系统中，需要保护系统位置、速度等敏感数据不被泄露，保护车辆不被非授权改装，以及保护车辆不因为系统参数被篡改而发生事故。其最终目标就是保护自动驾驶汽车正常运行。

物联网的安全需求

- 由于物联网存在特有的业务，因此物联网的安全需求与互联网不尽相同。

互联网业务示意图



物联网特有业务示意图

物联网安全需求

- 信息安全（互联网）考虑三个基本安全需求（CIA）：
  - **机密性（Confidentiality）**
  - **完整性（Integrity）**
  - **可用性（Availability）**
- 一些延伸的安全需求：
  - **真实性（Authenticity）**
  - **不可抵赖性（Non-Repudiation）**
  - **可问责性（Accountability）**
- 物联网安全挑战

三个基本安全需求

设备数量巨大	设备种类庞多	终端资源受限
⇩	⇩	⇩
数据量**剧增**	数据类型**多样**	算法**轻量级**

安全需求 – 机密性

- **机密性定义：**确保物联网敏感信息（设备数据、传感器数据、控制指令等）在采集、传输、存储和处理全生命周期中，仅能被授权主体访问的特性
- **互联网语义下**
  - 计算机存储数据、计算机之间通信数据
- **物联网语义下**
  - 物联网数据机密性考虑更多，如物联网数据反映的用户行为的机密性
  - 例子：
    - 智能电表的用电数据推测用户作息习惯
    - 智能设备传感器泄露用户语音、图像、位置、习惯等隐私

安全需求 – 完整性

- **完整性定义：**通过技术手段确物联网系统数据（控制指令、设备状态等）在采集、传输、存储和处理全过程中保持准确、完整且未被非法篡改的特性。

- **互联网语义下**
  - 计算机、服务器存储的数据的完整性，及计算机之间通信数据的完整性
  - 网络、服务器的系统完整性

- **物联网语义下**
  - **数据完整性：**数据量更大，数据类型更多，数据与用户行为关系紧密
  - **系统完整性**：物联网是多网络综合的产物，物联网系统更容易受到破坏，且后果直接威胁物理世界
  - 例子：云-管-边-端系统的完整性，尤其是端侧安全。

安全需求 – 可用性

- **可用性定义：**通过技术手段确保物联网系统及其服务在面临攻击、故障或异常状况时，仍能持续为授权用户提供可靠、及时服务的能力特性
- **互联网语义下**
  - 数据可用、业务可用
- **物联网语义下**
  - 数据可用性：与互联网中相似。
  - **业务可用性**：
    - **“业务耦合”**：物联网系统设计通常面向某个具体行业领域，如自动驾驶等。
    - **“有感有控”**：物联网能够通过执行器控制物理世界实体设备。
  - 因此，业务不可用将直接导致其关联的物理世界规则秩序被破坏。

Q：想想哪些攻击可以破坏数据或者系统可用性？

安全需求 – 真实性

- **真实性定义：**通过技术手段验证物联网系统中主体（设备、用户、服务）身份及数据来源合法可信的特性，确保操作行为和数据产生可精准溯源至授权实体。
- **互联网语义下**
  - 用户认证：即用户可被验证、可被信任
- **物联网语义下，认证对象、方法都发生变化：**
  - **对象**：除了用户认证，也关注设备认证、设备配对等。
  - **方法**：终端设备种类丰富、数量庞大、多元异构，认证方法要考虑轻量级及多种机制。

用户认证手段

物联网认证手段

安全需求 – 可问责性

- **可问责性定义：**通过技术机制确保物联网系统中所有操作行为可追踪、可审计，并能将安全事件定位至责任主体的特性。
- 系统的绝对安全是一个不可达到的目标，因此需要将破坏安全的行为**追溯到责任方**，以便于后续的责任追溯以及纠纷解除。
- 可问责性通常需要保证**不可抵赖性。**
- 物联网中的可问责性需求与互联网类似。

物联网中各安全需求的新挑战

安全需求	物联网中的新挑战
机密性 (Confidentiality)	1. 数据量大、类型多、与用户行为联系紧密； 2. 资源受限的物联网终端需要**轻量级的加密算法**。
完整性 (Integrity)	1. 数据量大、类型多、与用户行为联系紧密； 2. 物联网包含多种类型的网络，系统庞大复杂。
可用性 (Availability)	破坏物联网业务可用性可直接扰乱真实世界的秩序。
真实性 (Authenticity)	物联网设备数量巨大、种类丰富、资源受限，导致**认证对象、方法不同**，存在新的挑战。
可问责性 (Accountability)	与互联网类似。

物联网安全事件 – 机密性

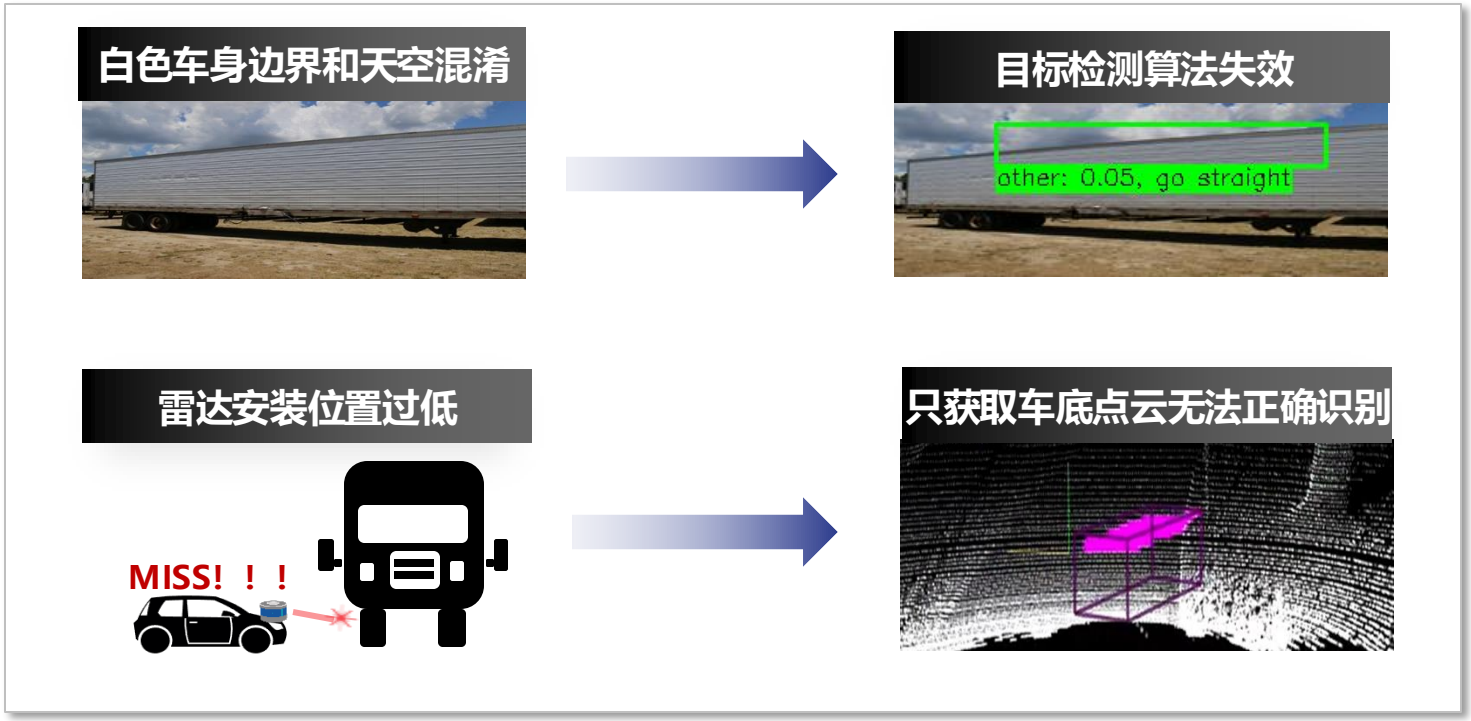
- 2017年3月，Spiral Toys玩具**数据遭到泄露**，泄露的敏感信息包括玩具的录音、220万账户的语音信息、MongoDB的数据等。
- 2017年8月，深圳某公司制造的17.5万个**物联网安防摄像头**被曝很容易就可被利用，只需使用**默认凭证**登陆就可访问摄像头的转播画面。
- 2023年，美国基因检测巨头23andMe近700万用户数据泄露，包括扎克伯格、马斯克和谷歌创始人谢尔盖·布林等。

分析:

- **物联网设备量大、数据量大**
- **传感器数量多，数据模态多样、隐私敏感**
- **机密性保护措施弱**

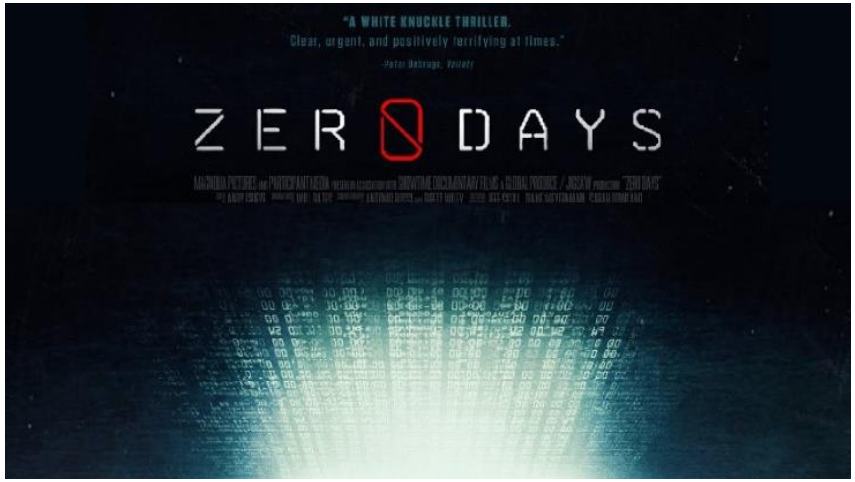
物联网安全事件 – 可用性

- **Tesla全球第一起自动驾驶致死事故**
  - 2016年5月7日，一辆启用半自动驾驶（Autopilot）功能的特斯拉电动汽车与一辆大型卡车相撞，司机在事故中丧生。Autopilot**没有检测到**卡车的白色侧面，物联网**感知功能**的错误可直接威胁真实世界。



物联网安全事件 – 可用性

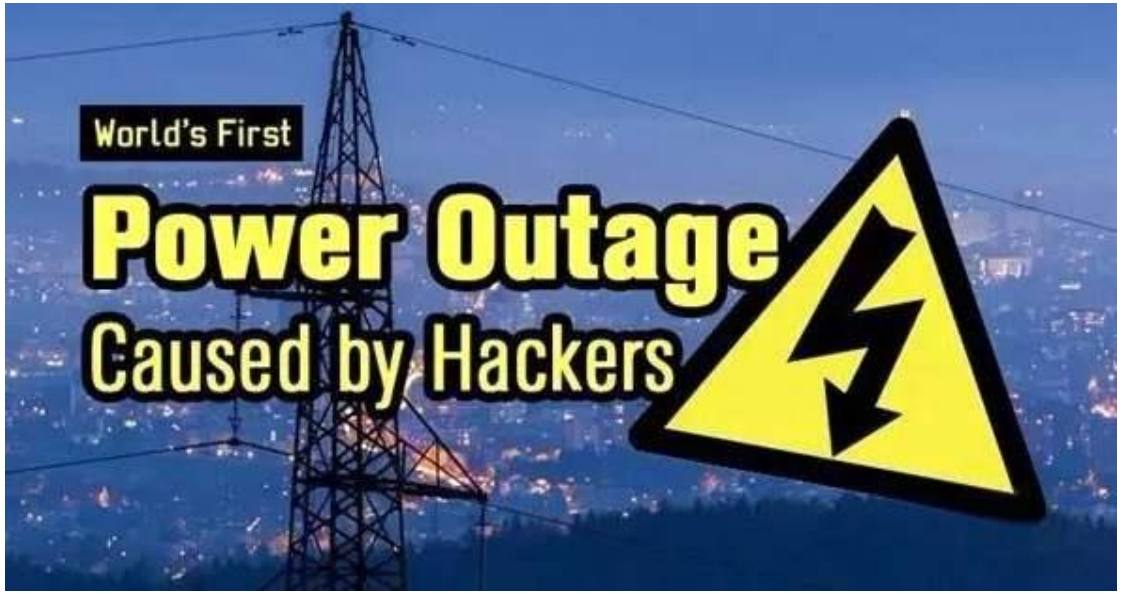
- “震网”病毒 – 伊朗核电站事件
  - Stuxnet蠕虫用于定向攻击基础（能源）设施，如国家电网、核电站、水坝水利设施等都是该病毒的攻击目标。
  - 全球已有约4.5万个网络被感染，其中60%主机位于伊朗境内 。伊朗政府已经确认核设施遭到攻击，导致铀浓缩离心机受损。



推荐观看：震网病毒纪录片：ZERO DAYS

物联网安全事件 – 可用性

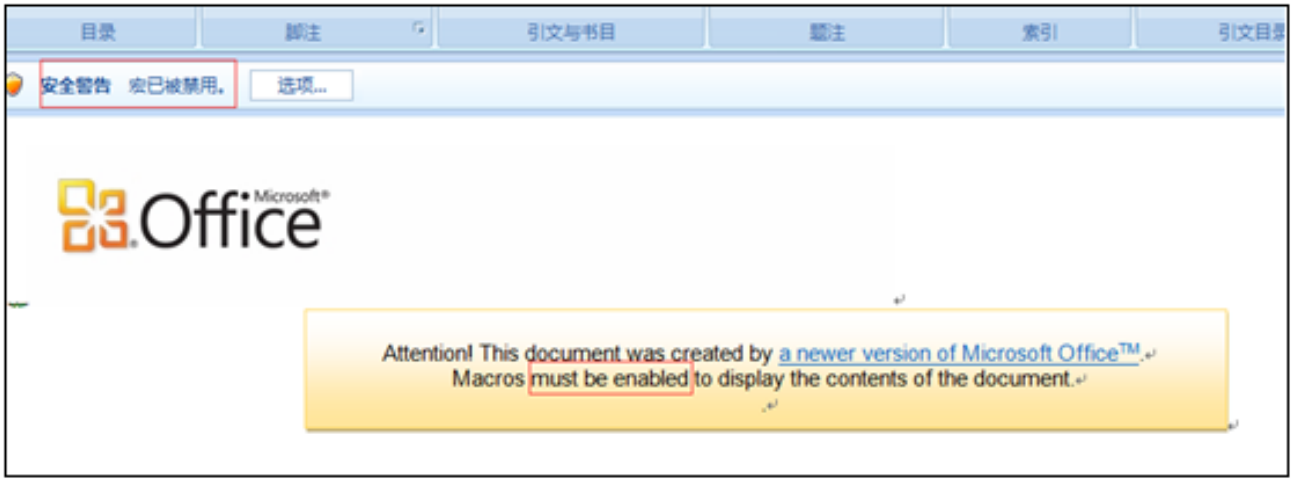
- **BlackEnergy – 乌克兰停电事件**
  - 2015年12月23日，乌克兰电力部门遭受到恶意代码攻击，导致了八万用户数小时的停电事故。
  - 电力：基础设施的基础



世界第一起由黑客引起的停电事件

物联网安全事件 – 可用性

- 攻击者向乌克兰电力公司发送了一封**钓鱼邮件**，该邮件中的文档被嵌入了恶意的**宏代码**，用户打开文档并运行宏，其操作系统就会被感染。
- 然后攻击者就可以对电力公司的网络资产进行探测以及横向移动，并最终获得**SCADA系统**的控制能力。攻击者在获得了SCADA系统的控制能力后，通过相关方法下达断电指令导致断电。
- **宏病毒**：一种依赖文档宏功能传播的恶意程序，主要针对Microsoft Office及同类办公软件的VBA（Visual Basic for Applications）开发环境，当用户启用宏（如点击"启用内容"），病毒激活



Microsoft Office宏病毒

物联网安全事件 – 可用性

- **增加恢复难度**：
  - 攻击者采用**覆盖MBR和部分扇区**方式，使系统重启后不能自举（如加电自检和磁盘引导等），阻止断电后的迅速恢复；
  - 采用**清除系统日志**的方式提升事件后续分析难度；
  - 采用**覆盖文件**的方式，导致实质性的数据损失。
- 与此同时，在线下还对电力客服中心进行电话DDoS攻击，从而不能有效推动恢复工作。

启示：针对物联网的**攻击需要结合业务**的特性才能能够造成严重后果。

同理，在物联网的安全**防护机制设计**中，应结合业务的特点。

第二节

物联网安全威胁

物联网安全威胁

- **定义**：指存在于环境、能力、行动或事件中可能会破坏安全并造成伤害的安全隐患，也就是说，威胁可能利用脆弱性并造成损失。

- 从架构上看，物联网有着“**云-管-边-端**”的架构，各层都可能存在软硬件缺陷、系统集成缺陷、管理环节缺陷等，均是潜在的**攻击入口**。因此，需要对各层安全威胁进行分析。

- 深入理解威胁是设计有针对性防护对策并最大限度保障安全的前提。

Q：你能列举下物联网的安全威胁有哪些吗？

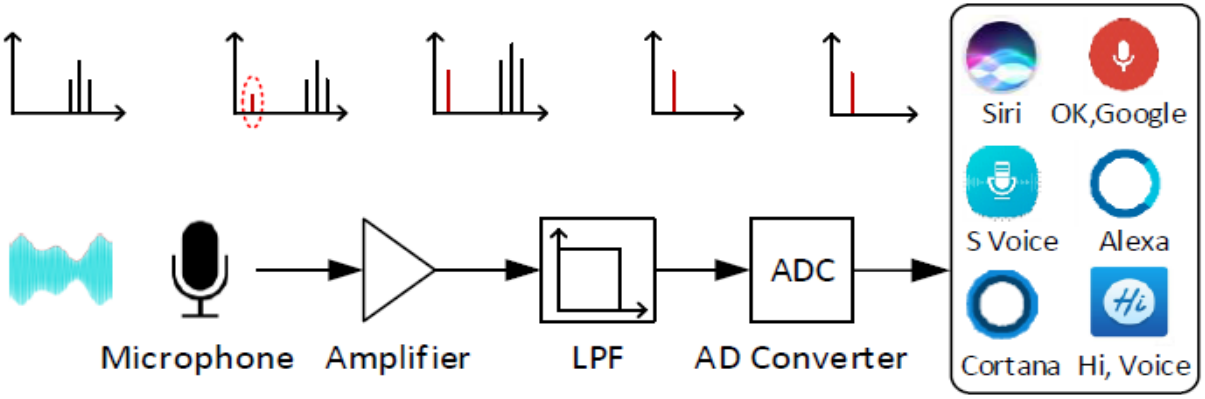
“端” 的安全威胁

1. 感控安全威胁：

- **传感器**：利用换能装置将物理信号转换为电信号
- **执行器**：将电信号转化为物理空间上的位移或旋转量

威胁：易受到**恶意物理信号**攻击，如拒绝服务攻击、欺骗攻击等

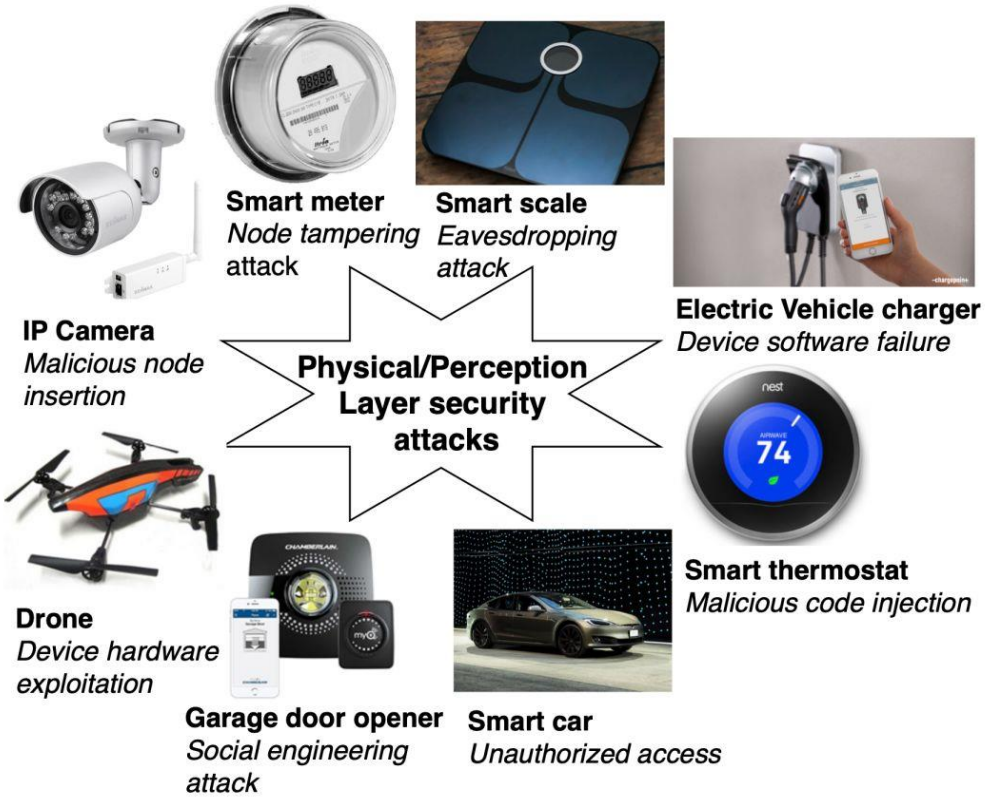
- 例如，海豚音攻击就是一种典型利用**超声信号**实现对终端麦克风传感器感测攻击的案例



海豚音攻击示意图

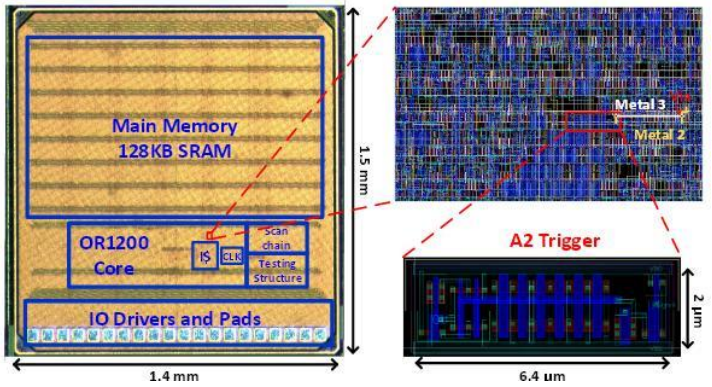
“端” 的安全威胁

2. **认证安全威胁**：物联网面临**恶意终端非法接入**的威胁
   - 终端软硬件海量异构、部署环境开放、设备资源受限，物联网设备身份认证提出新挑战



“端” 的安全威胁

3. **硬件安全威胁**：终端设备的硬件的核心组件是各类芯片，包括微处理器、微控制器、射频芯片、存储芯片等。芯片层的安全问题往往更加**危险且难以发现。**
   - 针对芯片的威胁：硬件木马、边信道攻击、乱序执行和预测执行漏洞、Rowhammer攻击等。



硬件后门

如：黎巴嫩爆炸的BP机事件

“端” 的安全威胁

4. **软件安全威胁**：物联网终端的软件包括固件、操作系统、各类应用实现等，软件本身可能存在安全问题，如软件逆向和软件漏洞。另外，攻击者通过**植入木马、病毒**等手段，可导致设备拒绝服务，获取设备控制权限甚至大规模控制网络。

- **软件逆向问题**
  - 固件获取
  - 固件逆向
- **软件漏洞问题**
  - 输入验证漏洞
  - 逻辑错误漏洞
  - 内存破坏漏洞
  - ……

“边” 的安全威胁

- **“边”定义：具备数据处理能力的边缘设备**

- 物联网的“边”面临“端”面临的所有安全威胁，包括感控安全、认证安全、硬件安全和软件安全等威胁。

- **特有威胁：**
  - **边缘节点劫持**：控制大量下游终端设备
  - **物理抵近攻击**：各类侧信道攻击等
  - **边缘AI隐私窃取**：终端模型窃取攻击等
  - Edge-LLM security

“管” 的安全威胁

- **“管”定义：数据传输的通道**

- 主要由三个部分构成：**协议**、**信道**和**流量**。
  - **协议安全威胁**
    - 协议是指数据（和信令）交换的规范、时序以及在发送和接收时对数据采取的操作。
    - 中间人攻击、协议逆向攻击、重放攻击等。
  - **信道安全威胁**
    - 信道指的是数据传输的媒介，如各类无线射频信号。
    - 窃听攻击、干扰攻击等。
  - **流量安全威胁**
    - 流量指的是特定时间内通信管道中传输的数据总量。
    - 拒绝服务攻击、隐私窃取等

第三节

物联网安全特点

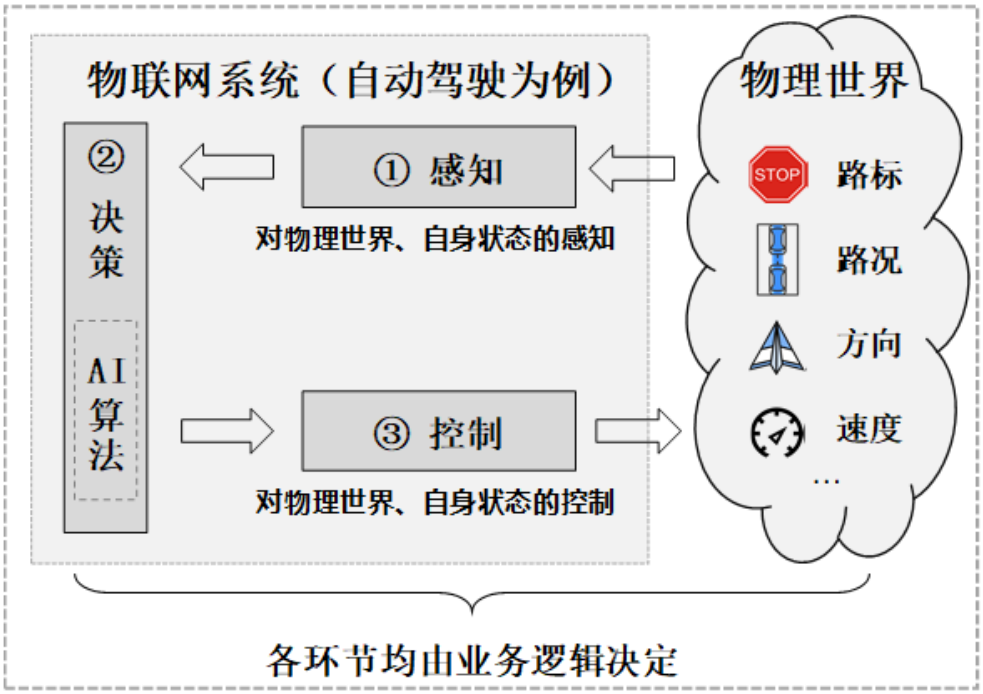
物联网安全特点：功能环节

- 物联网信息流及功能环节反应了物联网与互联网、传感网等其他网络的区别
- **感知：**各类传感器对环境和自身状态进行感知
- **决策：**决策单元利用AI等算法处理数据，并做出决策
- **控制：**控制单元下达相应控制指令并由相应的执行装置执行

物联网信息流

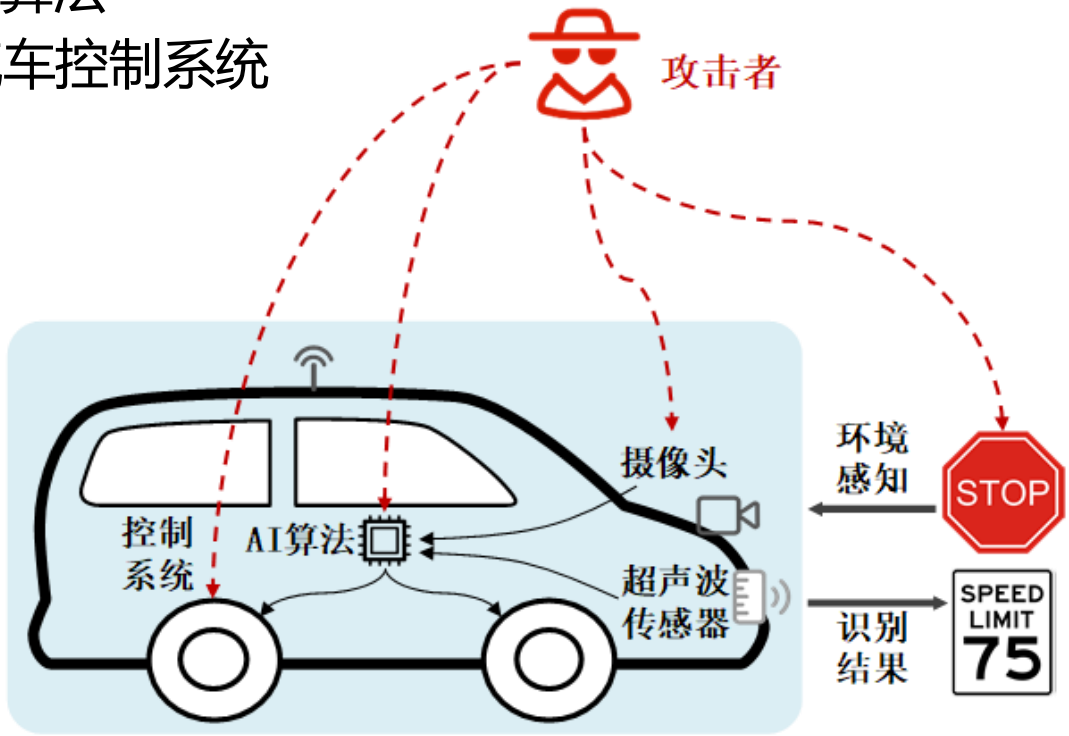
与功能环节

自动驾驶汽车为例



物联网安全特点：功能环节

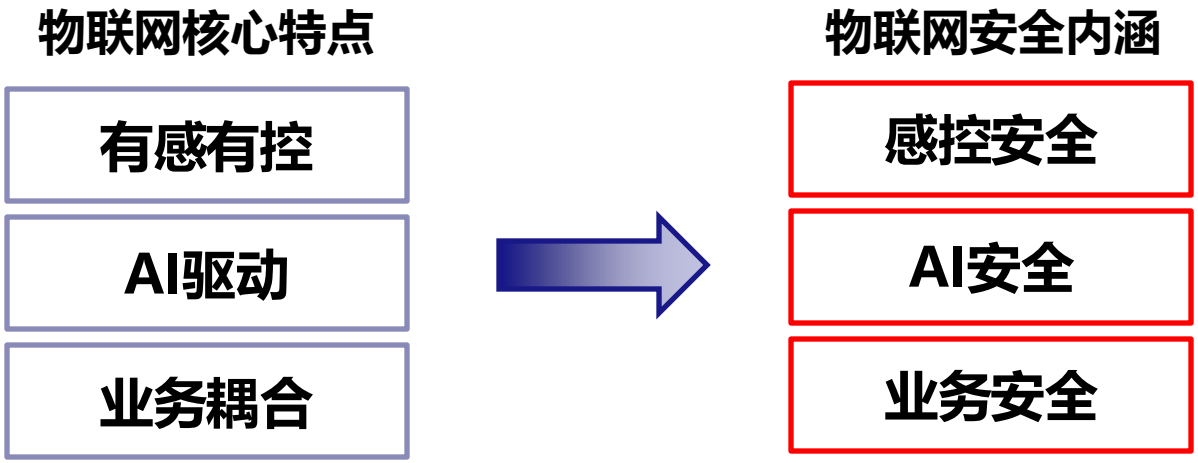
- 攻击者可以针对所有功能模块实施攻击：
  1. **物理世界**：如交通标志
  2. **感知**：如摄像头、超声波传感器
  3. **决策**：AI算法
  4. **控制**：汽车控制系统
  5. ……



以自动驾驶汽车为例

物联网安全特点

- 根据上述分析，可以总结如下：



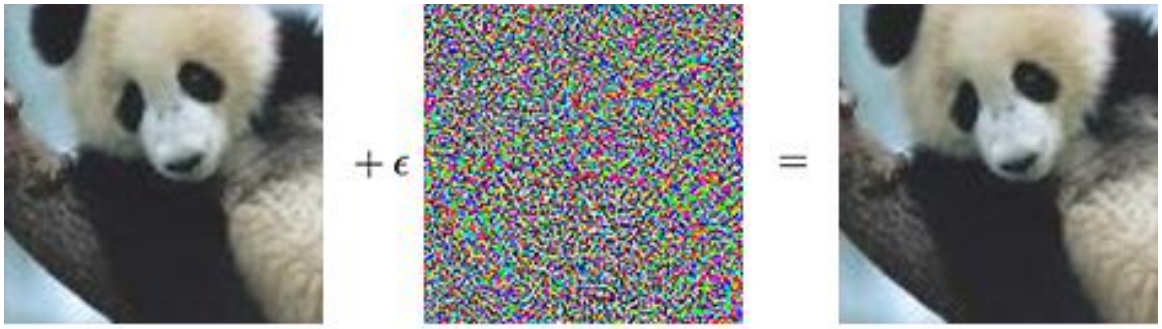
- **总结：**物联网安全特点和物联网特点紧密相关，体现了物联网和互联网的差异性，也是信息安全CIA模型的综合体现

特点一：感控安全

- **感知安全风险**
  - 传感器所测量的结果不能准确反映被测物理量，传感器存在脆弱性且容易被外部物理信号干扰
  - 脆弱性存在部位：换能器、信号处理电路等
  - 典型代表：信号超限、跨场感测等
- **控制安全风险**
  - 根据测量结果和用户需求进行控制是物联网的重要特性和实现功能的体现，同时也是物联网与互联网的重要区别
  - 控制安全：
    - Case1: 执行器接收到错误控制指令
    - Case2: 执行器接收到正确指令，执行动作错误

特点二：AI安全

- **“AI驱动”**是物联网智能化过程中的一大核心特点，同时AI也成为物联网的攻击面之一。
- AI安全**根本原因**：人工智能算法存在可被攻击者利用的脆弱性，典型攻击包括：数据中毒攻击、对抗样本攻击、逆向工程攻击。
- 大模型（LLM）加持之后，具身智能安全对物理世界危害更大



对抗样本攻击

(Adversarial Example)

特点三：业务安全

- **“业务耦合”**是物联网又一核心特点。
- **“业务”定义**：物联网系统为实现某一目标而进行感知、决策、控制等一系列工作时所执行的事务流程，是物联网的固有属性。
- **“业务安全”定义**：(1) 实体设备和系统运行符合设定规则和约束条件，(2) 规则和约束的制定符合实际逻辑、能达成预期目标。
- 从“震网”病毒、乌克兰大停电等安全事件中可知：
  - 针对业务逻辑的**恶意攻击**更有效、隐蔽，更具破坏性。
  - 要有效地实施**安全防护**，则必须从业务着手。

特点三：业务安全

- **例子**：电力物联网中的远程开合闸的业务安全
  - **符合时序规则**：远程操作员发布开/合指令，指令通过通信数据包传送给RTU等远动终端，远动终端I/O口输出高电平（或低电平、上升沿、下降沿等，不同终端自行设置），继电器通/断电状态改变，断路器开/合
  - **满足约束条件**：开合过程远动终端、继电器、断路器等设备**不受损坏**，断路器动作速率**不超出合理范围**
  - **指令合法合理**：不能出现未定义指令

断路器业务攻击

本章小结

- 物联网安全定义、安全核心术语定义
- 物联网相关安全事件分析
- “云-管-边-端”各层存在的典型性安全威胁
- 物联网安全三大特点：
  - **感控安全**
  - **AI安全**
  - **业务安全**

电影片段：Who Am I 我是谁：没有绝对安全的系统

推荐阅读

- 震网病毒分析
  - https://www.youtube.com/watch?v=J07N1KXOyfk
  - https://cyberhoot.com/cybrary/stuxnet/
- 乌克兰Black Energy大停电攻击
  - 《Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid》
- 电影：
  - 震网病毒纪录片《Zero days》
  - 《Who Am I 我是谁：没有绝对安全的系统》