聚力·引领
软件安全学术论坛

智慧城市中的应用与数据安全

陆宝华

雄安新区智能城市安全顾问
福州市首席网络安全专家
贵阳大数据与网络安全攻防演练技术总策划

聚力·引领
软件安全学术论坛

目录Catalog

雄安！智能城市！

01.

安全概述

聚力·引领

软件安全学术论坛

我们存在着两大类的安全问题

天灾！人祸！

对于网络安全Cyber Space Security，我们主要关注的是人祸，而对于一个智能城市来说，仅关注人祸是不够的。

对于人祸，我们的核心任务是：保证正确的授权操作

操作经过授权、授权是正确的、正确授权机制是有保障的。

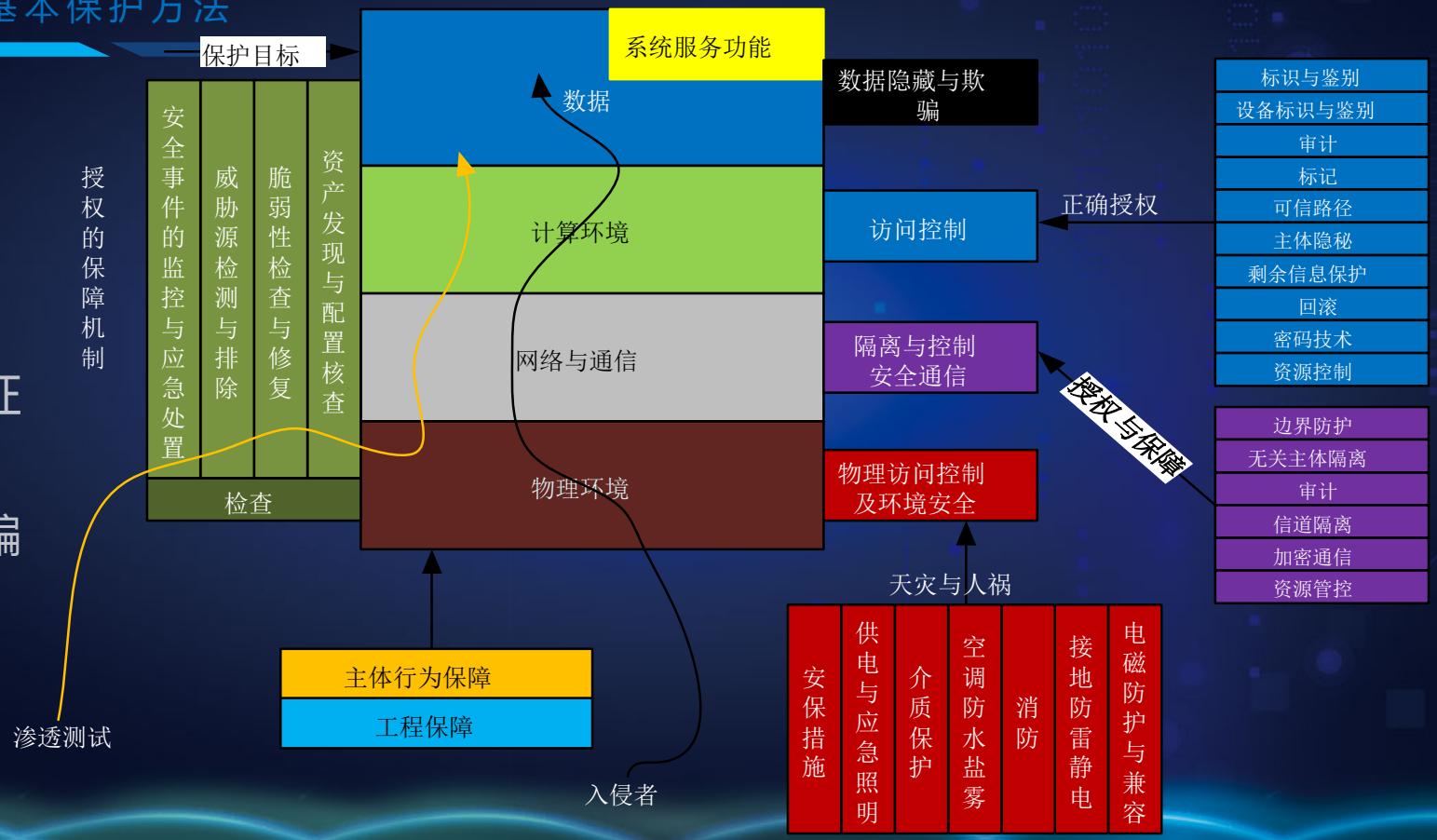
网络安全的基本保护方法

隔离

控制

检查验证

隐藏欺骗



应用程序的安全检查、监控特别重要

从近些年来报导的情况来看，系统软件的漏洞已经不是很多了，大量的漏洞多出在应用程序中，原因是应用软件开发的团队，安全开发能力参差不齐。

1、许多开发团队为了控制成本提高速度，经常会使用一些脚本程序，或者是直接调用一些成品模块。而这些程序中存在着大量的安全漏洞。

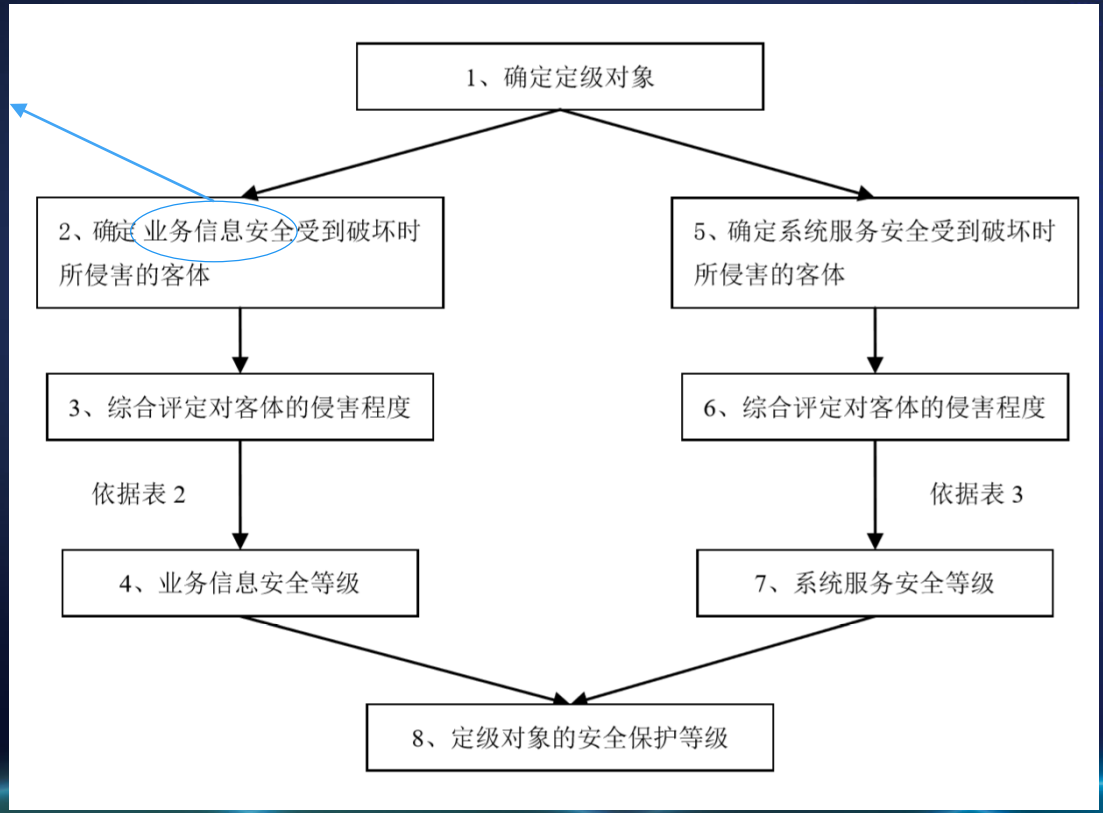
2、开发过程缺少安全控制，甚至有一些恶意人员会在程序中安装后门；

3、代码缺少审查，通过检测的程序与安装的程序并不是同一个版本。

传统安全的保护目标

业务信息安全 和 系统服务安全

数据安全



数据是网络与信息系统中第一重要的资产

智能城市的安全目标

02.

物联网导致的风险

聚力·引领

软件安全学术论坛

物联网所导致的风险

RFID的安全

可复制
数据库数据可篡改
泄露

卫星定位与导航

地面干扰

摄像头的安全

被控制

信号的安全

实时可用性
完整性
被人为破坏或篡改
环境安全
元器件失效

03.

大数据导致的风险

聚力·引领

软件安全学术论坛

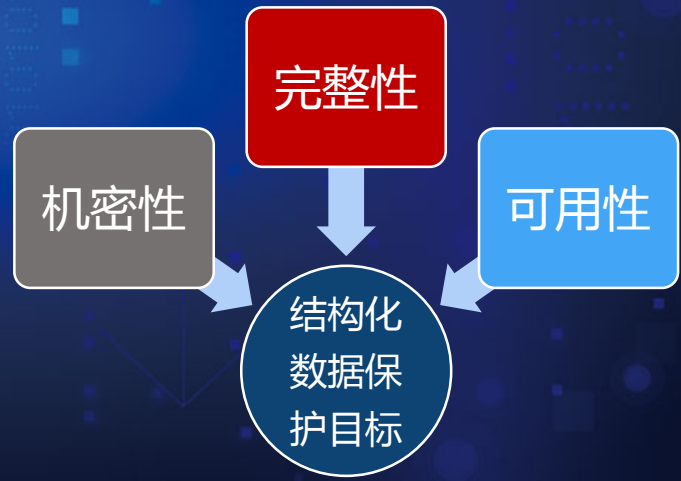
大数据导致的风险

智慧来源于数据，数据越丰富，产生的智慧就会更多更高级，但是同样大数据是需要保护的

结构化数据的保护：

保护其安全属性（机密性、完整性、可用性）；

根据实际安全需求，确定结构化数据的保护强度。

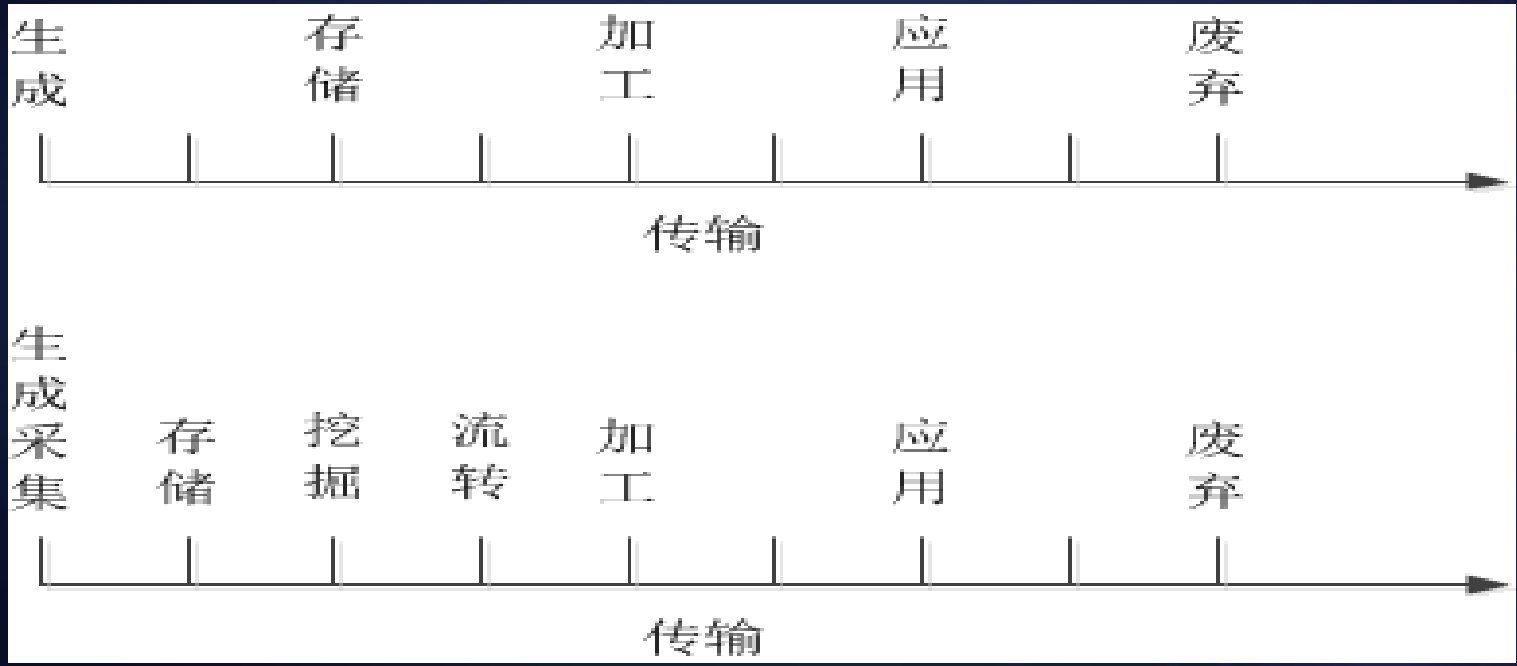


非结构化数据的含义

非结构化数据是数据结构不规则或不完整，没有预定义的数据模型，不方便用数据库二维逻辑表来表现的数据。包括所有格式的办公文档、文本、图片、XML, HTML、各类报表、图像和音频/视频信息等。对于这类数据，我们一般直接整体进行存储，而且一般存储为二进制的数据格式。

特点：格式多样，标准多样。

	传统数据	大数据
数据格式	结构化数据	非结构化数据+结构化数据
存储模式	集中存储	分布式存储
计算平台	数据库查询平台有较好的安全机制	分布式计算处理平台几乎没有安全机制
复杂度	相对简单	由于异构性，导致复杂度增加
计算物理环境	以服务器为主，有向云上转移的趋势有较清晰的边界	云是主要的承载物理平台，但仍有利用物理服务器，边界模糊
保护目标	机密性、完整性、可用性	机密性、完整性、可用性同时要考虑对数据真实性的确认
数据库结构	SQL	SQL+NOSQL
软件栈	C++为主	Java为主
主流规模	1～10台	3～1000台，最高可支持上万台
包含的内容	集中存储、查询	存储、查询、计算、ETL、分布式应用程序协调服务


生成
存储
加工
应用
废弃
传输
生成采集
存储
挖掘
流转
加工
应用
废弃
传输

大数据全生命周期的安全分析

大数据的安全需求

所有的网络安全需求

数据的真实性问题

挖掘中的访问控制问题

国家秘密的泄露与个人隐私泄露问题

元数据与源数据的错位问题

全生命周期中数据的溯源问题

大数据平台的安全问题

大数据的滥用（越权采集，越权挖掘，越权使用等）

大数据交易中的安全问题

大数据的跟踪问题

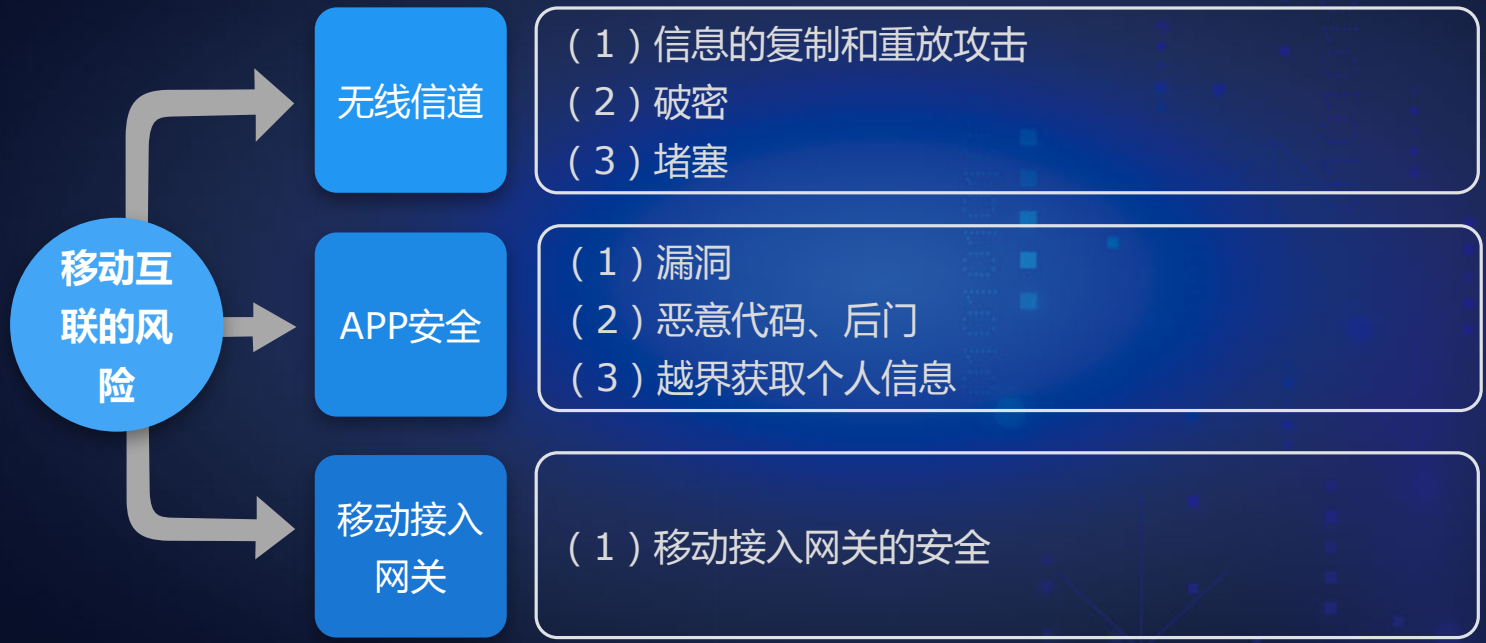
04.

移动互联的风险

聚力·引领

软件安全学术论坛

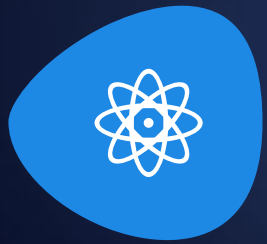
移动互联的风险


移动互联的风险
无线信道
（1）信息的复制和重放攻击
（2）破密
（3）堵塞
APP安全
（1）漏洞
（2）恶意代码、后门
（3）越界获取个人信息
移动接入网关
（1）移动接入网关的安全

05.
人工智能的风险

聚力·引领
软件安全学术论坛

人工智能的风险



人工智能（Artificial Intelligence），英文缩写为AI。人工智能是以计算机科学为基础，从智能的实质出发，生产出一种新的能以人类智能相似的方式做出反应的智能机器，该领域的研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等。

人工智能是以数据为基础的 ，但是仅有数据还不能构建人工智能系统，能够思维、判断、并能作出决策，将是人工智能的高级目标

人工智能的风险

美国智库"新美国安全中心"最近发布《人工智能：每个决策者需要知道什么》报告，提示人工智能的一些弱点可能对国家安全等领域造成巨大影响。

第一：脆弱性。目前的AI还是低级"思考"。

第二：不可预测性。

第三：弱可解释性。

第四：安全问题和漏洞。

第五：系统事故。

第六：人机交互失败。

第七：机器学习漏洞可被对手利用。

AI技术目前还在起步阶段，很多风险还并没有显露出来，各种科幻小说中给出的风险，未必不存在！

感谢您的聆听

THANK YOU FOR LISTENING

聚力·引领

软件安全学术论坛