2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

构建安全可信的智慧城市终端体系

主讲人：李华生

目 录

Contents

智慧城市与智能终端

Intelligent City and Terminals

- 智慧城市的全球规划
- 智慧城市体系下的智能终端

智慧城市的全球规划

斯德哥尔摩
智慧交通体系

纽约
新一代水资源管理

苏塞克斯县

里约热内卢
城市运营中心

维也纳
数据服务智慧决策

马斯达尔城
二氧化碳零排放

新加坡
“电子政府2015”

首尔
U-City

横滨
i-Japan2015战略

布里斯班
“绿心智慧城市计划”

中国的智慧城市及应用场景

数字乌鲁木齐

“分建共享”突破数据整合之困

智慧北京

智能融合和信息应用

数字长春

土地资源的三维管理

数字济南

市政管理服务民生

智慧重庆

应用广泛深入 移动便携唱主角

智慧上海

三维地理信息服务智慧城市建设

智慧深圳

完善、优质和高效的地理空间数据服务

数字苏州

完善、优质和高效的地理空间数据服务

智慧厦门

推动行业的社会化应用

智慧宁波

国内首个真正落地的云地理服务平台

智慧城市的通用体系结构

智慧城市体系下的感知终端

智能终端的安全风险

Risk of Intelligent Terminals

- 已发生的安全事件
- 智能终端本身的安全风险
- 智能终端沦陷后的扩大风险

智能终端被攻击的安全事件

【智能警报使得300万辆汽车易受到黑客攻击】

分类：资讯 | 发表于 2019年3月8日 星期五 下午 9:19　　发表评论

【智能警报使得300万辆汽车易受到黑客攻击】据外媒报道，两款颇受欢迎的智能汽车报警系统存全缺陷，这使得潜在的黑客能够跟踪车辆，打开车门，在某些情况下还能切断引擎。这些问题是在最大的两家智能汽车报警器制造商Viper和Pandora Car alarm System生产的报警系统中发现的。品牌拥有多达300万的客户，生产的高端设备价格高达数千美元。

智能网联汽车信息安全报告：海豚音竟然也成了攻击手段

来源：geekcar　编辑：廖海玲　2018-04-08 10:41　浏览量：9374

随着汽车产业正在不断的发展，汽车中增加了更多的便利和个性化的驾驶体验。消费者希望汽车和生活不断地加以连接，这也推动了汽车制造商增加车辆和个人设备之间的整合，如和智能手机等。

入侵特斯拉——智能汽车安全性分析

摘要：特斯拉汽车一直受到黑客的关注，很多安全研究人员都尝试过挖掘特斯拉汽车的漏洞，主要原因是特斯拉是纯电并且有网络连接，可以通过网络对汽车进行控制，而且特斯拉本身也非常依赖电子控制系统。本文就来分析特斯拉已经的问题。

家庭摄像头正在遭受攻击！你需要绝对的安全感

2018-04-19 20:39　摄像头

当心智能门锁、无线摄像头被攻击！物联网设备漏洞正逐年增加

光明网
18-01-22　13:56

【当心智能门锁、无线摄像头被攻击！物联网设备漏洞正逐年增加】智能门锁遭破解、无线摄像头泄露隐私、劫持智能对讲机……由安恒信息、中国科学院计算技术研究所INSIGHT　TEAM、中国电子信息产业发展研究院联合编撰《2017年度网络空间安全报告》显示，物联网安全已成为威胁网络安全的

智能终端的网络安全风险





智能终端　　安全风险

风险：
1、弱口令
2、已知漏洞未修复

风险：
重放攻击，获取指纹
或者解锁指令

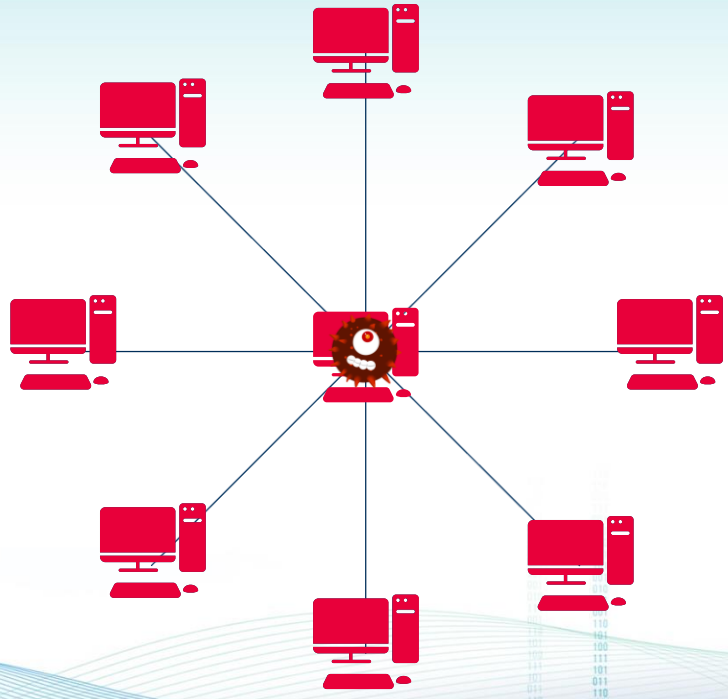
风险：
1、木马植入
2、流量劫持

风险：
1、漏洞层出不穷
2、遥控指令攻击

风险：
1、车载系统沦陷
2、CAN控制器沦陷

智能终端沦陷后的扩大风险

- 智能终端作为肉鸡参与DDOS攻击
- 智能终端作为感染源攻击内网数据中心
- 智能终端作为传播源，感染同一网络的其他终端
- 智能终端作为入口控制关键基础设施



可信终端体系的新思路

- 智能终端防御上的困境
- 新思路1：去中心化的自治区方案
- 新思路2：以区块链技术为基础的威胁检测方案
- 新思路3：以“安全心”为基础的主动防御方案

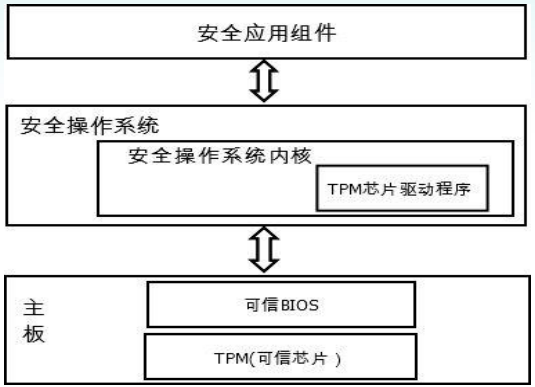
智能终端防御上的困境

传统技术

1、杀病毒、防火墙、入侵检测的传统“老三样”难以应对针对智能终端的新型攻击。

2、重型方案也无法在智能终端上落地。

TPM技术

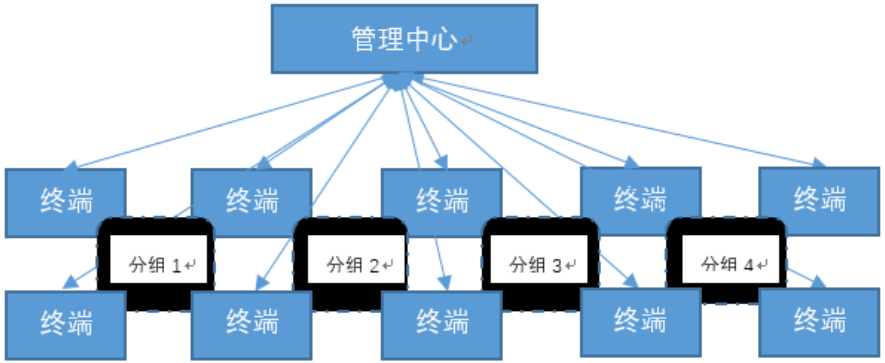


1、基于内置硬件模块，技术还有待成熟。

2、其经济成本也是待攻克难题。

新思路1：去中心化的自治区方案

去中心化的自治区方案



□ **一种物联网场景下去中心化的异常终端发现方法及装置** 【公开】

申请号：CN201810640246

申请日：2018.06.21

公开（公告）号：CN108900488A

公开（公告）日：2018.11.27

IPC分类号：H04L29/06；

申请（专利权）人：杭州安恒信息技术股份有限公司；

发明人：李华生；范渊；黄进；

1、智能终端自动分组。

2、智能终端分组动态调整。

3、智能终端组内自动判别异常行为，找出不可信终端。

4、智能终端组内自动处置异常终端，处置不可信终端。

新思路2：以区块链技术为基础的威胁检测方案

☐ 一种基于区块链的轻量物联网终端系统及其控制方法 【公开】

申请号：CN201811224065

申请日：2018.10.19

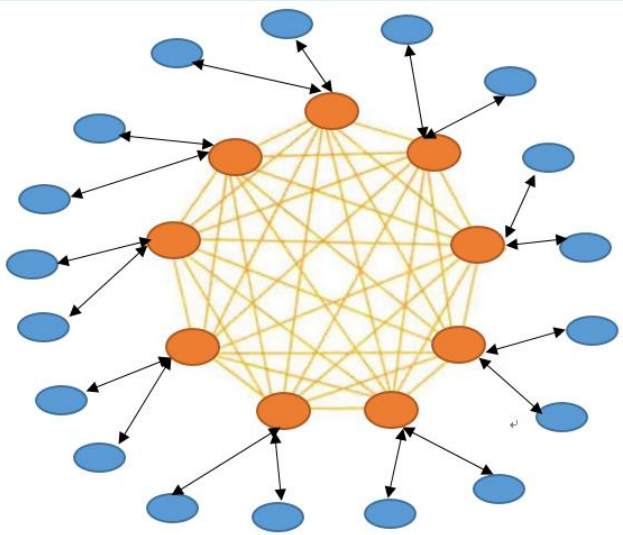
公开（公告）号：CN109388968A

公开（公告）日：2019.02.26

IPC分类号：G06F21/62；

申请（专利权）人：杭州安恒信息技术股份有限公司；

发明人：李华生；范渊；



1、智能终端节点自动加入就近的区块链节点。

2、区块链节点接收威胁信息。

3、区块链节点交换威胁信息，并本地决策威胁行为。

4、智能终端接收区块链节点的安全策略，并实现威胁处置。

新思路3：以“安全心”为基础的主动防御方案

IOT-SH

智能终端内生“安全心”

防御心 → 恶意文件免疫引擎
恶意流量免疫引擎
信道加密

感知心 → 恶意行为识别与记录
感知邻居设备安全状态

协同心 → 感知协同引擎共享情报
感知协同引擎共享策略

新思路3：“安全心”的恶意文件免疫引擎工作原理

恶意文件免疫引擎

进程1

进程2

进程3

进程4

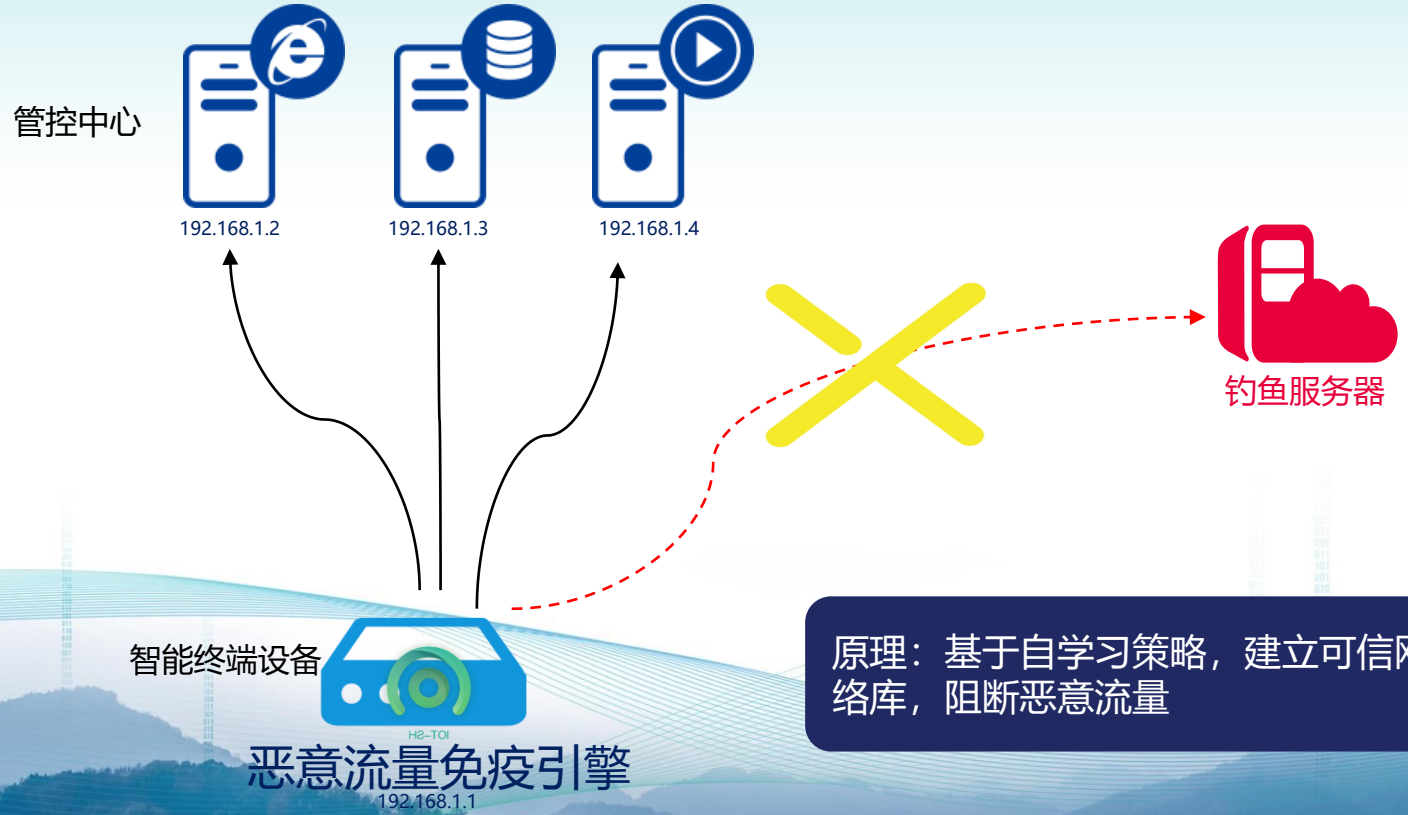
进程5

进程6

恶意文件

原理：基于自学习策略，建立可信文件库，阻断恶意文件

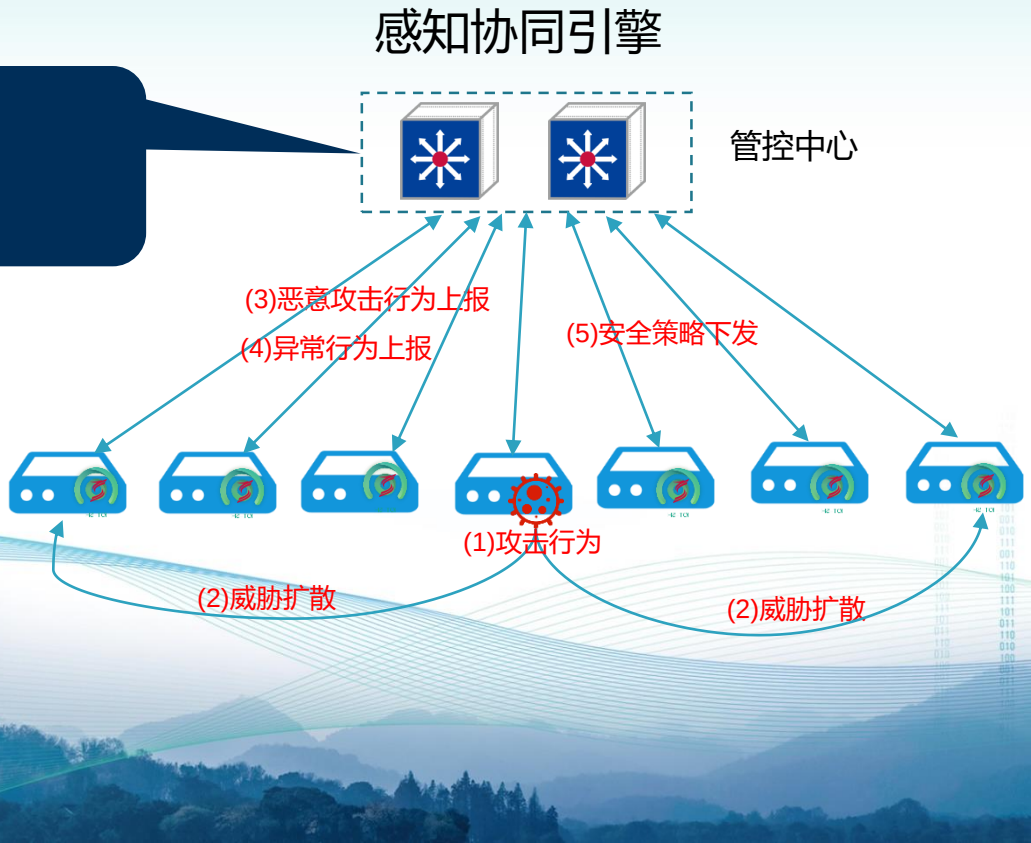
新思路3：“安全心” 的恶意流量免疫引擎工作原理



原理：基于自学习策略，建立可信网络库，阻断恶意流量

新思路3：“安全心”的感知协同引擎

1、接收威胁数据
2、确认恶意行为
3、形成全网策略
4、全网态势感知



THANK YOU

谢　　谢　　观　　看