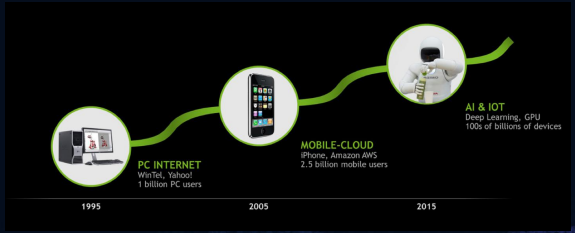
有AI, 更安全

沈鹏飞　百度安全事业部副总经理

时代趋势


PC INTERNET
WinTel, Yahoo!
1 billion PC users
MOBILE-CLOUD
iPhone, Amazon AWS
2.5 billion mobile users
AI & IOT
Deep Learning, GPU
100s of billions of devices
1995
2005
2015

智能变革

AI城市，全面感知，全局决策，
实时调控，根治交通拥堵

农业AI化，种好中国粮

人工智能、大数据、云计算（ABC）驱动下的
组织·制度·经济变革

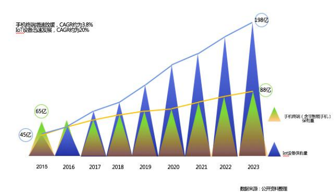
医疗AI化，智能问诊、基因分析、
精准医疗，新药研发

智慧家居，AI更懂你

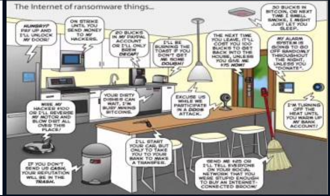
智慧警务，打击溯源，全网无死角

AI激活制造业，智能供应链，释放
人力，产业与组织模式的变革

万物互联



手机终端增速放缓，CAGR约为3.8%
IoT设备迅速发展，CAGR约为20%
198亿
88亿
65亿
45亿
2015
2016
2017
2018
2019
2020
2021
2022
2023
手机终端（含非智能手机）保有量
IoT设备保有量
数据来源：公开资料整理



The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

新的挑战

人身安全

- 智能驾驶
- 工业物联网
- 智能机器人

数据安全与隐私

- 云计算
- 智能家居
- 数据供应链

AI决策安全

- 可靠性
- 可解释性
- 伦理性


EAGLE
ROBOT

安全隐私

智能终端设备被用于隐私勒索\欺诈\薅羊毛\APT基础设施\DDoS...
Mirai僵尸网络：摄像头，峰值1.5 Tbps，造成美国大面积断网
Rowdy僵尸网络：Mirai家族，感染有线电视机顶盒

2017年10月，国外安全研究人员发现某品牌家居设备中存在的安全的漏洞，可导致包括冰箱、干衣机、洗碗机、微波炉以及吸尘器机器人在内的各种家电设备被远程控制

山东大学生宋振宇电信诈骗猝死案
广东惠来女大学生电信诈骗自杀案
摄像头侵犯隐私案，涉案QQ群组及号码达5000余个

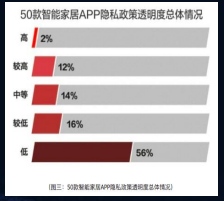
GeekPwn极棒国际安全极客大赛历届，连续破解各种类型IoT设备，包括大量智能家居设备

2018年2月，美国《消费者安全报告》显示，数百万的智能电视存在安全漏洞，攻击者可以通过这些漏洞操控电视机，播放冒犯性视频，或者安装不需要的应用程序

APP 隐私

（图一：50款智能家居APP隐私政策透明度红榜）

（图二：50款智能家居APP隐私政策透明度黑榜）

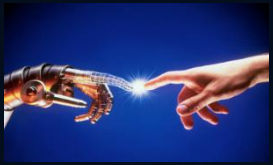


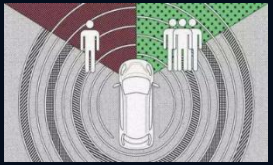
（图三：50款智能家居APP隐私政策透明度总体情况）

据南方都市报近期发布的《智能家居隐私政策透明度测评报告》显示，50款APP中，22款智能家居APP没有隐私政策，仅7款APP在隐私政策，提及个人敏感信息。值得注意的是，由智能家居设备带来的隐私安全问题不容回避。

2018-08-11 08:42

安全伦理





难度要点

生态链复杂

设备上运行的软件来自产业链各个环节
每个环节都存在大量的安全问题
问题层出不穷，快速响应能力很重要
能否从根本上消除安全漏洞？

设备碎片化

设备种类及软件版本繁多
逐个处理安全问题成本很高
安全防护需要有高适应性

新的攻防维度

AI攻防
如何提升AI本身的安全性？

难度要点

生态链复杂

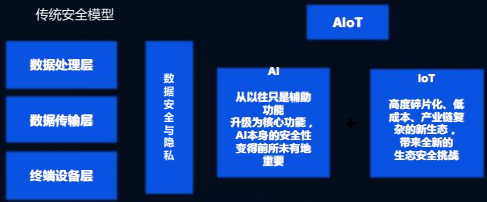
设备上运行的软件来自产业链各个环节
每个环节都存在大量的安全问题
问题层出不穷，快速响应能力很重要
能否从根本上消除安全漏洞？

设备碎片化

设备种类及软件版本繁多
逐个处理安全问题成本很高
安全防护需要有高适应性

新的攻防维度

AI攻防
如何提升AI本身的安全性？



威胁攻击

	远程设备攻击	传输劫持	云端攻击	人工智能攻击
安全隐患	缺乏控制校验 “后门”功能 系统漏洞	传输未加密 传输层漏洞	云服务漏洞 缺乏攻击防护	缺乏对抗能力 本地AI模型无保护
攻击手段	木马攻击 局域网内远程攻击 广域网远程攻击 近场攻击	中间人攻击	分布式拒绝服务 攻击 服务器入侵	AI对抗攻击 AI模型分析
攻击后果	远程非法控制设备	隐私窃取 信息篡改 升级过程劫持	业务不可用 非法控制云端 数据窃取及篡改	非法控制AI决策 AI知识产权窃取

FIT 2019

百度安全开放矩阵
共建AI新时代开放生态

百度安全
有AI更安全

三大支点

技术赋能

- 百度安全开源技术矩阵，全面解决云管端、大数据和算法层面的一系列安全风险问题，助力整个AI生态

标准驱动

- 借助产业生态商业场景，实现安全标准与产业的紧密结合，推动产业的快速规模化发展

生态共建

- 联合终端厂商、安全厂商、高校专家和科研机构的力量，将安全能力对外开放给生态合作伙伴，共同应对AI时代面临的各种安全问题

百度安全
有AI更安全

OASES

生态矩阵

生态层

学术、企业、政府、机构
多层面开放协作

联合开放实验室
威胁情报矩阵助力智慧警务
安全人才培养

伪基站定位识别系统
网址安全检测系统
IP地址风险画像
反电信诈骗系统
SMS短信内容安全检测系统

平台层

开放行业解决方案

智能终端
安全解决方案

智能车机
安全解决方案

基础层

开源技术矩阵

Baidu AI Security Stack (BASS)

下一代人工智能安全技术栈

云管端+大数据+
算法

有AI，更安全

快速
响应

持续对抗

全面开源

生态矩阵

生态层

学术、企业、政府、机构
多层面开放协作

联合开放实验室
威胁情报矩阵助力智慧警务
安全人才培养

伪基站定位识别系统
网址安全检测系统
IP地址风险画像
反电信诈骗系统
SMS短信内容安全检测系统

平台层

开放行业解决方案

智能终端
安全解决方案

智能车机
安全解决方案

基础层

开源技术矩阵

Baidu AI Security Stack (BASS)

下一代人工智能安全技术栈

云管端+大数据+
算法

有AI，更安全

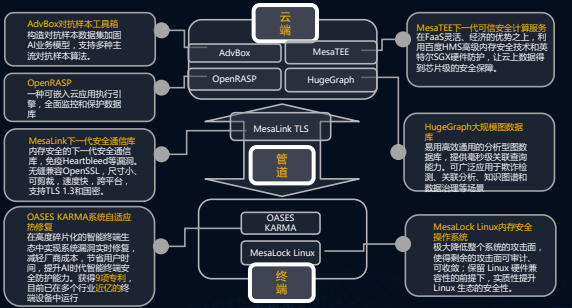
快速
响应

持续对抗

全面开源

BASS

FIT 2019



Baidu AI Security Stack (BASS)

下一代人工智能安全技术栈

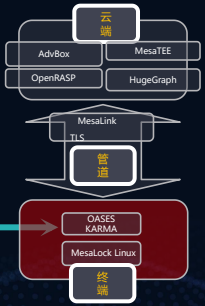
KARMA

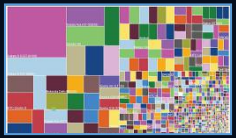
FIT 2019

OASES KARMA系统自适应热修复

在高度碎片化的智能终端生态中实现系统漏洞实时修复，减轻厂商成本，节省用户时间，提升AI时代智能终端安全防护能力。

业界首创，获得9项专利，曾两相国际顶级安全会议BlackHat与USENIX。目前已在多个行业近亿的终端设备中运行

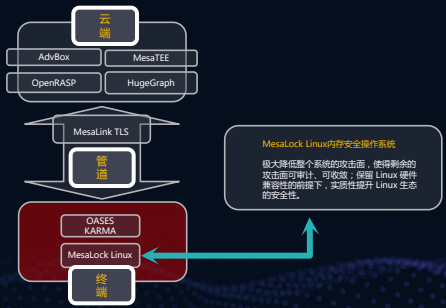




Baidu AI Security Stack (BASS)
下一代人工智能安全技术栈

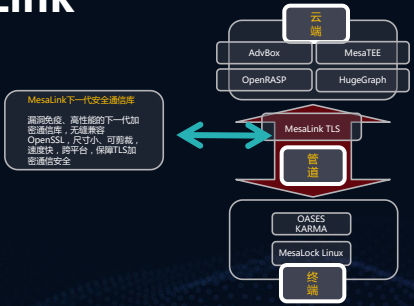
Mesalock Linux

Baidu AI Security Stack (BASS)
下一代人工智能安全技术栈



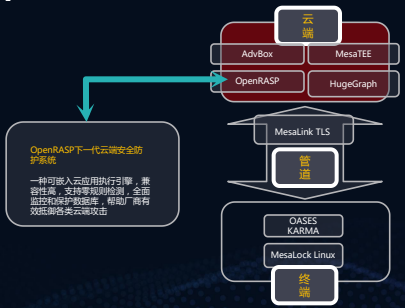
MesaLink

FIT 2019



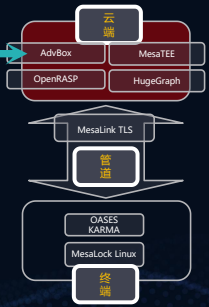
Baidu AI Security Stack (BASS)
下一代人工智能安全技术栈

OpenRASP



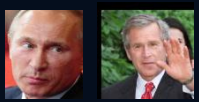
Baidu AI Security Stack (BASS)
下一代人工智能安全技术栈

AdvBox



AdvBox对抗样本工具箱

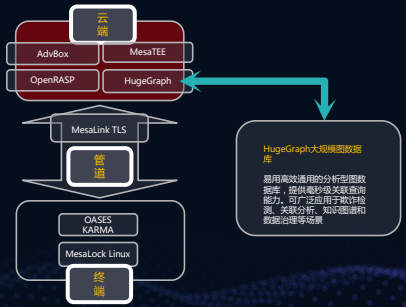
国内首个AI攻防工具箱，高效使用最新的生成方法构造对抗样本数据集，用于对抗样本的特征统计、攻击全新的AI应用，加固业务AI模型，支持PaddlePaddle、Caffe2、Keras、TensorFlow等主流深度学习平台，帮助厂商提升AI算法的健壮性



Baidu AI Security Stack (BASS)
下一代人工智能安全技术栈

HugeGraph

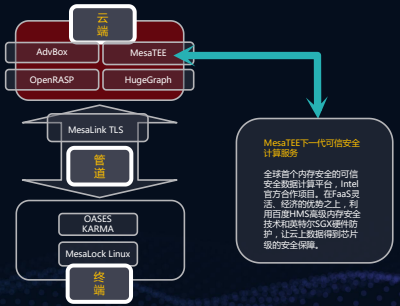
Baidu AI Security Stack (BASS)
下一代人工智能安全技术栈



MesaTEE

FIT 2019

Baidu AI Security Stack (BASS)
下一代人工智能安全技术栈



生态矩阵

生态层
学术、企业、政府、机构
多层面开放协作

联合开放实验室
威胁情报矩阵助力智慧警务
安全人才培养

伪基站定位识别系统
网址安全检测系统
IP地址风险画像
反电信诈骗系统
SMS短信内容安全检测系统

平台层
开放行业解决方案

智能终端
安全解决方案

智能车机
安全解决方案

基础层
开源技术矩阵

Baidu AI Security Stack (BASS)

下一代人工智能安全技术栈

云管端+大数据
+算法

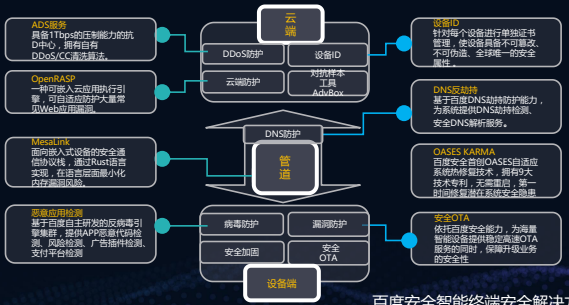
有AI 更安全

快速
响应

持续
对抗

全面开
源

解决方案



百度安全智能终端安全解决方案

生态联盟

OASES（ Open AI Sys-tEm Security ）智能终端安全生态联盟

由百度、信通院、华为联合发起成立

成员包括智能终端厂商、安全厂商、国内外知名高校、行业安全专家等等；目前成员单位30家，联盟为邀请制注册。

30+生态伙伴 ¦ 覆盖多个行业超过1亿+ 智能设备

生态联盟

OASES（ Open AI Sys-tEm Security ）智能终端安全生态联盟

方案推广

协助安全厂商
推广安全方案

标准制定

制定相关安全技
术及测评标准

安全评测

进行各行业终端安
全评测及评比

2018年3月

发布国内首个智能电视行业安全报告

举办“智电视 安未来”智能电视安全技术沙龙

2018年6月

发布智能音箱安全评测行业报告

联合举办“AI智能音箱产业峰会”

2018年7月

完成OASES智能电视安全团体标准制定

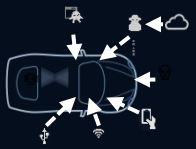
2018年10月

举办AIoT行业技术交流会

2018年11月

完成OASES智能音箱安全团体标准制定

智能车机



百度安全 apollo 汽车信息安全实验室

Scan 全面检测
执行车辆安全漏洞扫描及汽车信息安全评估，提供安全评估报告和修复方案

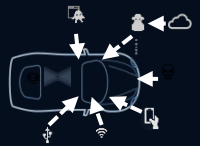
Shield 纵深防御
构建纵深安全防御体系，通过身份验证、区域隔离、访问控制等安全措施，及时发现并阻断安全威胁

See 安全可视
监控、检测车联连接情况，车辆安全状态以及网络攻击，基于百度大数据安全威胁分析，提供更准确的威胁态势和安全防护措施，与安全模块协同防御

Save 免召回
提供免召回应急修复机制，通过OASES热修复及OTA升级，及时对车辆进行安全加固

智能终端安全解决方案4S全生命周期安全保障

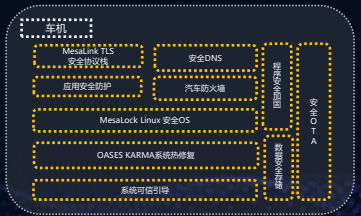
智能车机



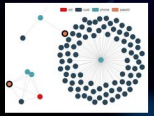
百度安全 apollo 汽车信息安全实验室

智能终端安全解决方案4S全生命周期安全保障

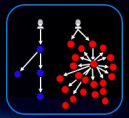
- 云安全
- 外部通信安全
- 内部通信安全
- 应用安全
- 操作系统安全
- 硬件安全
- 数据安全
- 手机终端安全



智慧警务



哪个设备的行为异常？

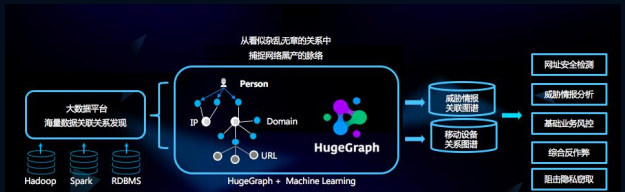


邀请好友领红包，揪出“薅羊毛党”

网络黑产的传播路径分析？

- 仅2018年上半年，处理全网145.4亿条有害信息
- 首创7*24小时智能建模，大数据分析和机器学习对恶意网址及变种精准拦截
- 2017年拦截窃取用户隐私恶意网址540万条
- 打击溯源，“滤网行动”中配合公安机关破获首例手机访客营销黑产

智慧警务



在百度安全协助公安机关破获的多起**电信诈骗、伪基站、流量劫持、用户隐私窃取**等重大黑产案件中，
提供了打击溯源的核心能力，全方位实现从数据整合到分析挖掘，助力智慧公安新业态

面向AIoT时代的安全

快速响应	漏洞免疫	保护隐私	端云一体	生态开源
自适应漏洞修复及安全防御体系，第一时间全面修复和缓解安全隐患	基于内存安全语言的系统核心组件，从根本上免疫二进制层面的漏洞	基于Intel SGX的内存安全可信计算，有效保护用户隐私数据安全	覆盖设备安全、传输安全、云端安全及AI安全，提供全方位安全防护	主要技术均已开源，安全更安心引领安全技术标准化，共建健康安全生态

智能家居

FIT 2019

设备安全防护

KARMA自适应系统热修复

业界首创的专利性动态修复技术
帮助厂商快速、低成本、一次性修复多种设备中的漏洞及功能缺陷
防御远程攻击及设备root

BOTA安全OTA

双向认证、升级包加密、防降级、安全传输等多重安全机制
保障OTA过程安全

程序加固

支持手机控制端App及设备端程序的加固
保障应用程序安全

MesaLock Linux

内存安全的嵌入式Linux OS

传输防护

MesaLink安全加密通信库

漏洞免疫、高性能的下一代加密通信库
保障TLS加密通信安全

XDNS DNS防护

基于业界最丰富的DNS数据积累与对抗经验保障DNS通信安全

云端防护

MesaTEE
云端数据防护

Intel官方合作项目
全球首个内存安全的可信安全数据计算平台
帮助厂商保护云端隐私及机密数据

OpenRASP
自适应云端安全防护

OWASP全球技术项目
开源，兼容性高，支持零规则检测
帮助厂商有效抵御各类云端攻击

人工智能防护

Advbox AI攻防工具箱

国内首个AI攻防工具集，支持各种主流DL平台
帮助厂商提升AI算法的健壮性

AI模型加固

基于MesaTEE及程序加固技术
保障云端及本地AI模型安全

智能家居


云端
Intel SGX TEE
Web应用服务器
MesaTEE云端数据及AI模型防护
OpenRASP自适应云端安全防护
平台、服务及工具
安全管理平台
加固平台及服务
AdvBox AI攻防工具箱
设备端(Android/Linux)
用户层
BASS用户层
XDNS DNS防护
MesaLink 安全加密通信库
KARMA 自适应系统热修复+远程攻击防护
BOTA 安全OTA
MesaLock Linux
内核层
BASS内核层
KARMA 自适应内核热修复+root防护

生态矩阵

生态层
学术、企业、政府、机构
多层面开放协作

联合开放实验室
威胁情报矩阵助力智慧警务
安全人才培养

- 伪基站定位识别系统
- 网址安全检测系统
- IP地址风险画像
- 反电信诈骗系统
- SMS短信内容安全检测系统

平台层
开放行业解决方案

- 智能终端 安全解决方案
- 智能车机 安全解决方案

基础层
开源技术矩阵

Baidu AI Security Stack (BASS)
下一代人工智能安全技术栈

- 云管端+大数据+算法
- 有AI 更安全
- 快速响应
- 持续对抗
- 全面开源

生态合作

锚定前沿技术与产业发展，开展联合开放实验室

- 深入多元化前沿科技产业链，与国内外学术企业机构开展前瞻性、针对性的研究合作 ：中科院、清华大学、复旦大学、南京大学、上海交大、信通院泰尔实验室、中科院软件研究所
- 联合清华大学经管学院发布《中国互联网安全现状研究报告》，聚焦网站和系统安全、关键基础设施安全、机构数据安全、物联网安全、云安全、AI安全六大安全议题

网络安全人才培养

- 将具有26年历史的国际极客大赛DEF CON首度引入中国，搭建中国安全企业、研究机构与国际交流合作的平台，为中国以及全球安全行业培育中坚力量、输送人才。
- 连续五年支持中国安全战队走向全球舞台、切磋技术，让立志于安全事业的年轻学子成为最大的受益者
- BSRC（百度安全应急响应中心）联手白帽子打造互联网安全蓝军

人工智能+智慧警务

- 与海南省公安厅在研究新型网络犯罪形式、打击黑色产业链、反电信诈骗等各个方面展开深入合作
- 配合北京市公安局海淀分局破获“手机访客营销”国内首例新型侵犯用户个人隐私黑产团伙
- 威胁情报矩阵助力智慧警务（伪基站、反电信诈骗、网址安全等）

写在最后

安全不是任何一家公司、一个社区、一个生态能够独立解决的事情，需要以更开放的态度，更广泛的合作与共享应对，在开放包容、多元互鉴中寻求共赢。

从PC到移动再到AI时代，科技发展的日新月异、万物互联，带来新的安全问题与攻击方式，也带来新的安全场景与机会。

“有AI，更安全”，如何运用AI做安全，AI时代需要更安全，安全的AI产品，百度安全在新的格局下全力布局AIOT，将思考变为最佳实践，为百度及整个业态赋能，集结所有安全圈的力量，与各界安全厂商通力合作与携手，共同为安全生态建设贡献力量，共同打造AI时代新型挑战下的诺亚方舟！

有Ai世界会更美好，我们是这个世界的蓝军！


FREEBUF | FIT
THANKS