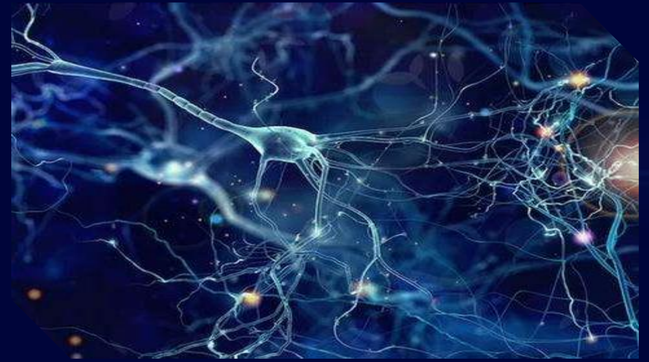
梆梆安全 BANGCLE | 稳如泰山 · 值得托付

2018 西湖论剑 · 网络安全大会
West Lake Cybersecurity Conference

智能之源 安全之本

阚志刚
梆梆安全CEO



通过感知外界信息并不断学习进化，人类产生了智能

基于大量数据的学习与训练，机器产生了智能

如果数据的**获取**出现了问题.....

- 微软 AI 聊天机器人 Tay 上线，发表的第一篇推文：向世界问好
- 之后不到24小时被紧急下架，因为其不断对网友骂脏话，发表大量不当言论
- 微软表示，没有对Tay交流中学习到的内容作任何限定

如果数据的**处理**出现了问题……

1989年，智能机器人棋手杀人事件

机器人棋手突然向金属棋盘释放出强电流，

将赢其三局前苏联国际象棋冠军击毙。

人工智能安全事件

2015年7月，工厂机器人杀人事件

德国大众汽车公司包纳塔尔工厂中的一个机器人杀死了一名人类工作人员。

数据

智能之源 安全之本

感知能力的全面增强

数据种类和数量均成爆发状态

物联网应用的全面普及

个人隐私数据面临巨大风险

对数据的利用与发掘

对社会及人类的发展影响深远

数据安全保护，从原点开始

微边界
安全战略

安全边界

互联网

无边界

云计算、移动互联网

微边界

物联网

在感知终端应用微边界保护架构

微边界安全多重防御架构

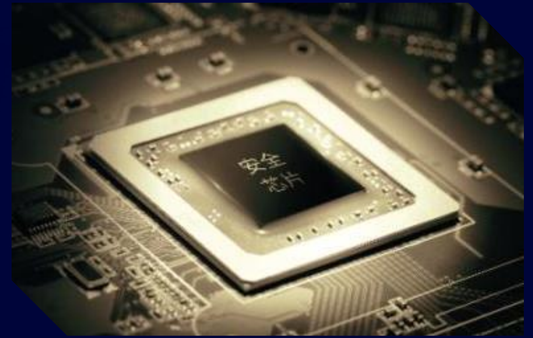
- **微边界**
  - 微边界防火墙
- **检测与审计**
  - 总线/控制网络
- **嵌入式系统**
  - 智能终端安全
  - 威胁预警系统
- **程序**
  - 程序加固
  - 代码混淆
- **资源文件**
  - 代码混淆
  - 完整性保护
- **数据/密钥**
  - 安全加密
  - 白盒保护

固件升级、应用程序升级、远程故障诊断排除

安全事件平台、安全威胁预警

安全启动

保护终端数据处理环境的安全



操作系统启动 → 任何操作系统加载代码 → BIOS

传统的BIOS启动

操作系统启动 → 认证的操作系统加载代码 → TPM

安全启动

程序保护

保护终端数据处理程序的安全

梆梆安全程序保护

程序安全—风险/问题

核心代码IP（算法）窃取

加密算法破解

控制协议、后台交互逻辑暴露

后台漏洞暴露

程序保护—加密/混淆

隐藏设计思路和细节

保护知识产权

抵抗各种攻击

防止漏洞挖掘和恶意利用

敏感信息保护

关键数据不泄露、不被非法访问

梆梆安全密钥白盒

在一个不可控的客户端环境下，实现安全的密钥存储

在一个不可信的客户端环境下，实现可信的逻辑计算

主动防御

终端数据风险实时监测与响应

梆梆安全终端预警系统

发现威胁

深入系统内核层威胁动态识别

- 实时监控系统内核层和应用层的异常行为，并实时预警；
- 针对终端系统和应用的行为做关联分析，发现深层次安全风险，准确定位安全威胁。

定位威胁

针对终端和应用的威胁实时定位

- 定位具体终端和应用存在的安全威胁。
- 定位应用某个进程存在威胁
- 定位攻击路径
- 定位威胁扩散范围

解决威胁

根据业务定制化安全防护策略

- **根据用户业务定制化安全防护策略，例如阻止恶意程序安装等**

移动APP中的数据

全方位保护移动数据的安全

移动APP
主要安全风险

移动应用篡改攻击
客户端动态注入
动态劫持攻击
不安全的数据存储
不足的服务器安全
传输层保护不足
非预期的数据泄露
脆弱的认证和授权
密码算法破解
缺乏二进制保护
钓鱼攻击
中间人攻击
键盘记录、屏幕录像
非信任输入

态势感知

提供全面的数据运营安全管理

基于终端数据构建安全态势感知平台

结合终端资产管理

- 自动识别终端，获取资产信息
- 快速查找和管理目标终端
- 支持群组管理

全网威胁态势感知

- 数据采集：智能终端、APP、流量
- 大数据分析
- 运维与应急响应

梆梆安全开启微边界数据保护时代，让智能更安全！

THANKS 谢谢观看