GoldenRiver

隐私保护与可信计算

谦川科技 COO 郭伟

May 2021

目录

万物互联世界的隐私场景

数据销毁 | 数据分享 | 数据使用 | 数据存储

数据传输

数据存储 | 数据收集

数据控制者

1010110
1001001
1101010

数据处理者

设备与连接管理 | 数据生命周期管理 | 数据分析 | 安全管理

数据采集终端

数据主体

智能家居

智慧城市

个人智能终端设备

物联网/智能汽车

隐私评估 | 法规遵从

数据治理 | 可信验证

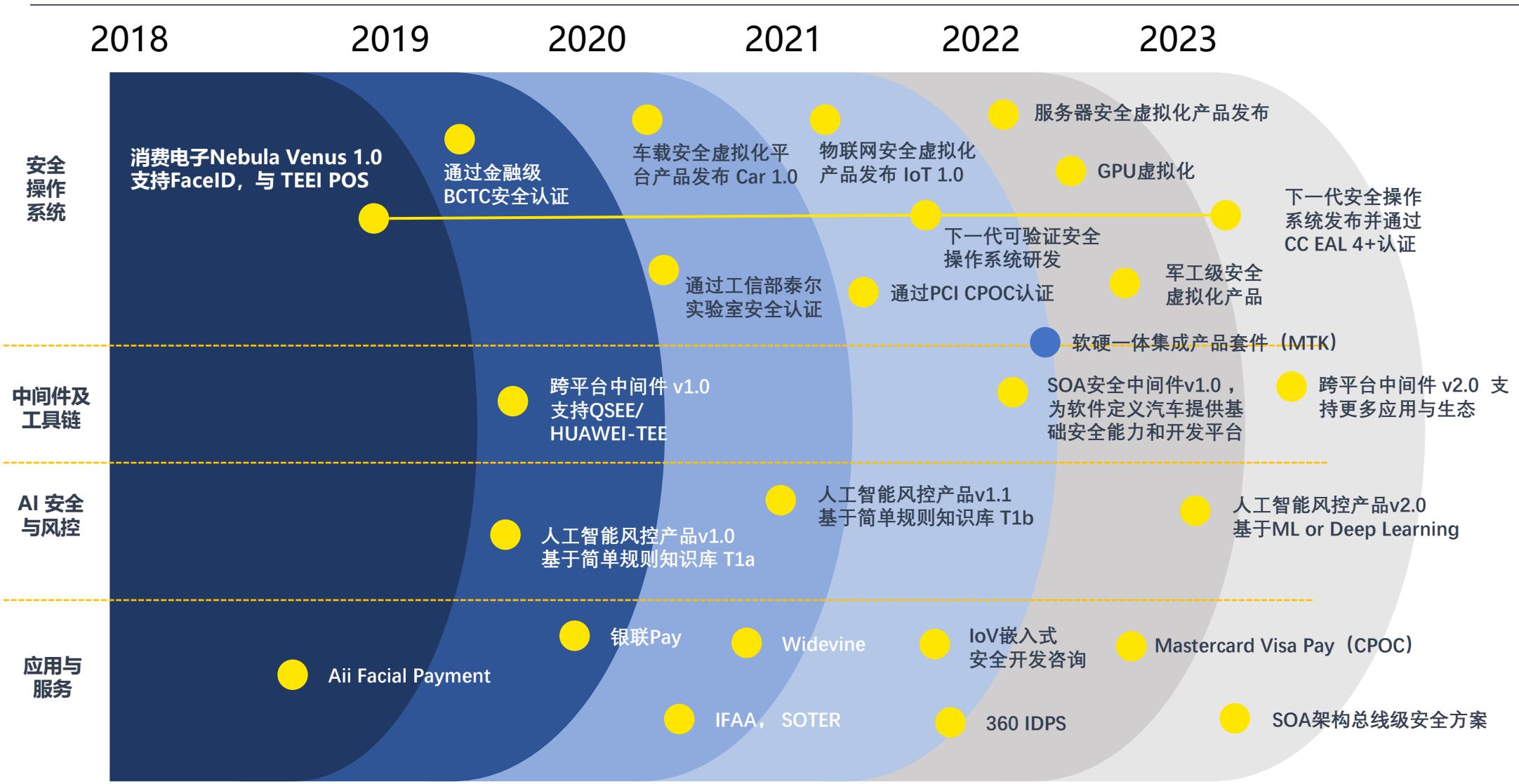
MPC/AL | 区块链

TEE | 可信应用

TEE（Trusted Execution Environment）：可信执行环境
MPC（Secure Multi-Party Computation）：多方安全计算
AL（Federated Learning）：联邦学习


终端可信计算产品方案
TEE/Hypervisor

产品线路图


2018
2019
2020
2021
2022
2023
安全操作系统
中间件及工具链
AI 安全与风控
应用与服务
消费电子Nebula Venus 1.0
支持FaceID，与 TEEI POS
通过金融级
BCTC安全认证
车载安全虚拟化平台产品发布 Car 1.0
物联网安全虚拟化产品发布 IoT 1.0
服务器安全虚拟化产品发布
GPU虚拟化
下一代安全操作系统发布并通过CC EAL 4+认证
下一代可验证安全操作系统研发
通过工信部泰尔实验室安全认证
通过PCI CPOC认证
军工级安全虚拟化产品
软硬一体集成产品套件（MTK）
跨平台中间件 v1.0
支持QSEE/
HUAWEI-TEE
SOA安全中间件v1.0，为软件定义汽车提供基础安全能力和开发平台
跨平台中间件 v2.0 支持更多应用与生态
人工智能风控产品v1.1
基于简单规则知识库 T1b
人工智能风控产品v1.0
基于简单规则知识库 T1a
人工智能风控产品v2.0
基于ML or Deep Learning
银联Pay
Widevine
IoV嵌入式安全开发咨询
Mastercard Visa Pay（CPOC）
Aii Facial Payment
IFAA，SOTER
360 IDPS
SOA架构总线级安全方案

产品功能描述
vTrust TEE OS

1 安全操作系统/内核

- 架构支持虚拟化的安全微内核；
- 内核/应用均支持64bit；
- 位置无关设计，可在4G以上任意地址段加载；
- 多核并发，多CA同时调用多TA；
- 多进程/多线程，同时调度；
- 时间空间隔离，多层级颗粒度权限控制；
- 关键模块形式化验证；
- Stack Guard；
- ALSR / KALSR；
- PXN / PAN；

2 安全系统服务

- 跨平台中间件，支持QSEE；
- 基于微内核能力集的安全应用管理器（OTrP）；
- 安全存储；
- 可信用户界面（TUI）；
- 设备风控，Android Root检测；
- Gate Keeper；
- Key Master；
- 安全摄像头；
- 安全NFC；

3 开发支持

- SDK，同时支持模拟器和真机开发；
- PDK，同时支持模拟器和真机开发；
- C/C++，支持POSIX；
- 支持TensorFlow / Pytorch等主流AI框架；

4 标准支持

- TEE/TUI满足TEE国标、央行TEE标准，以及银联TEEI 3.0标准；
- 设备风控满足国家PCI CPOC及银联设备风控标准；
- 安全NFC/安全摄像头，满足银联安全检测标准；

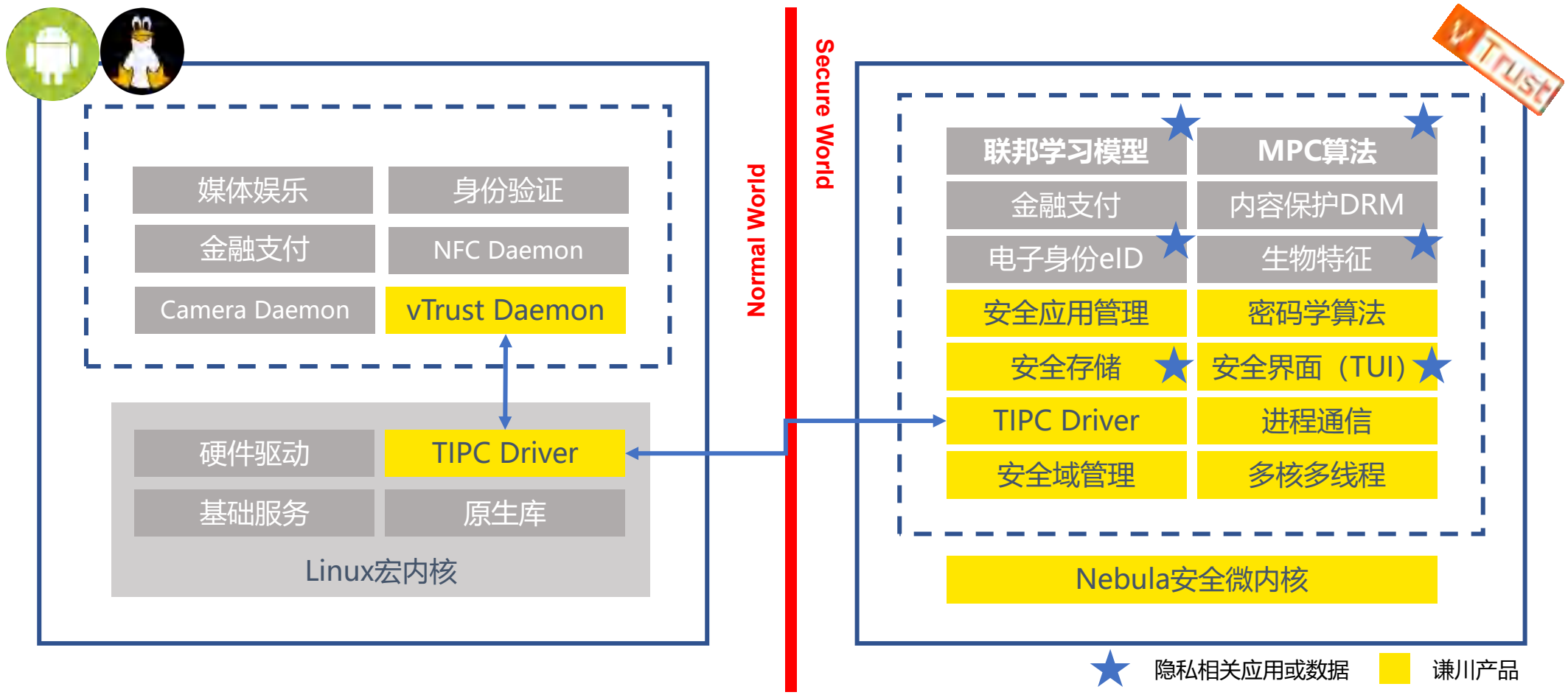
产品功能描述
T-Hyper

开发工具	SDK PDK- QEMU+cmdline			
工具链	Linaro/GNU Tool chain			
中间件 & libs	C,C++,BoriingSSL, Openmp, POSIX, IPv4/IPv6， USB host stack, device 2d, 3D, and OpenGL graphics， web services			
可移植性	支持应用程序从Linux、UNIX或其他开源程序的快速迁移			
Hypervisor	Guest主机的失效检测和重启	Guest主机的完整性检测	低开销	Virtual IO
	Virtual CPU model	根据优先级固定到核心或共享核心	带触发的共享内存	
安全性	最小Root操作	减少攻击面	内存地址随机化	安全存储/安全文件系统
	细粒度能力控制（最小权限）	沙箱	异常/完整性检测	内存保护
可靠性	容错性	自我修复	内存限制	
实时性	抢占式调度，在用户空间和内核空间都不屏蔽中断，TCB足够小，可以快速切换上下文			
多核支持	AMP, SMP, BMP			
架构	Secure Micro-Hypervisor			
认证	国标/央行/银联标准			

- 谦川T-Hyper嵌入式虚拟化平台，基于谦川Nebula微内核OS构建；
- 针对主流嵌入式SoC方案提供了丰富的底层技术支撑和安全机制；
- 良好的兼容性和可移植性，并提供完整的工具链和开发工具，确保快速开发迭代；
- 利用SDK/PDK开发上层应用，使得开发者可以将更多的关注点聚焦于自身业务，而无需考虑底层安全和硬件适配的问题；

利用vTrust构架智能终端隐私安全基座

ARM 芯片架构

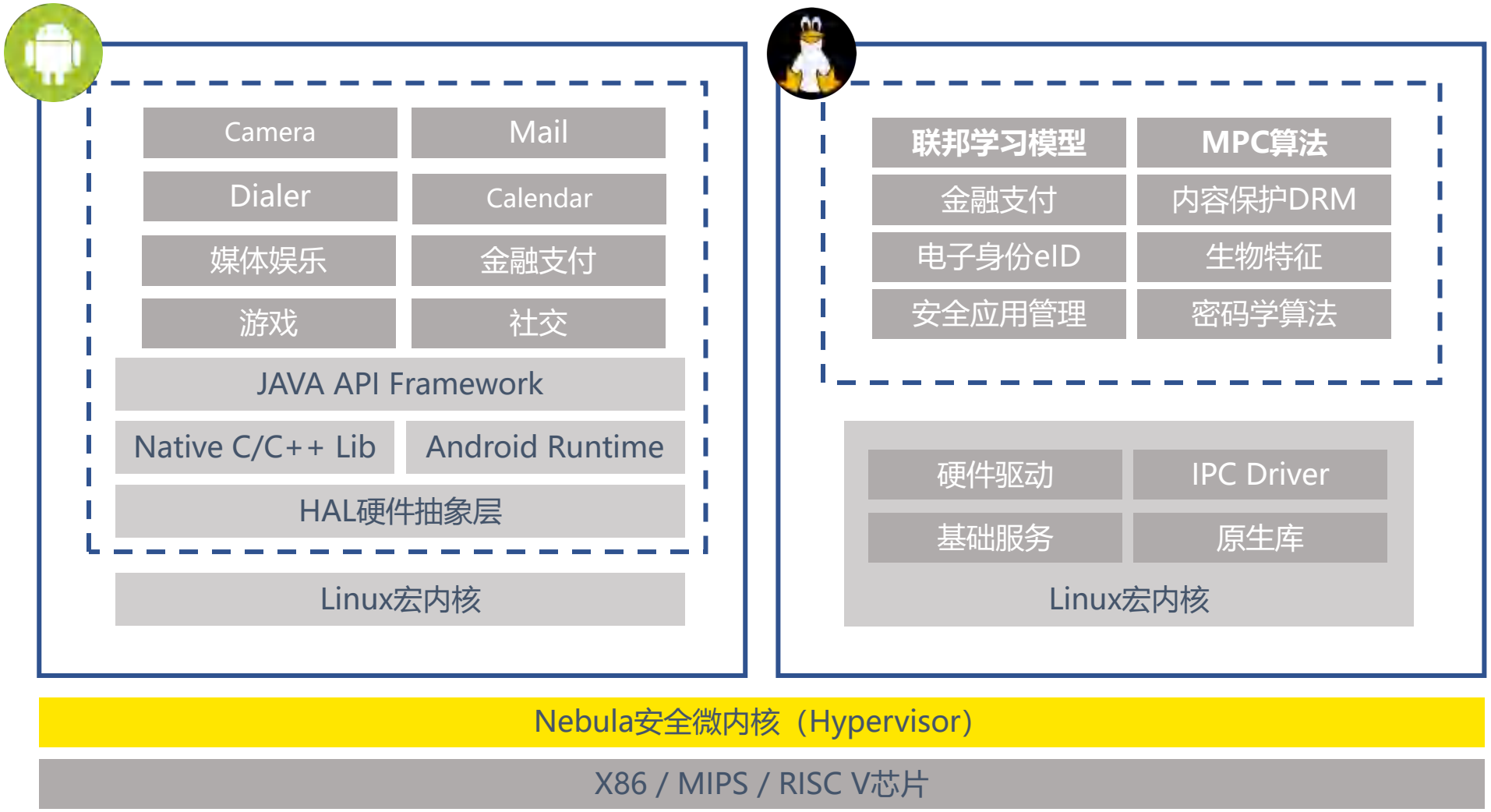


- Linux/Android系统无法提供硬件级别的隐私保护，并且由于层出不穷的内核漏洞，导致用户隐私数据可以被黑客通过技术手段获取；
- 常规APP可以调用vTrust Daemon，实现与TEE环境的通信，调用可信应用或隐私数据；

- TEE为联邦学习、MPC等隐私技术提供基于硬件的可信安全方案；
- 通过TUI安全界面，可以实现用户告知确认过程的安全防篡改，并留存可信的合规证据；
- 通过安全存储模块，可以对用户隐私数据进行块级加密存储，进一步确保隐私数据的安全；

利用T-Hyper构架智能终端隐私安全基座

X86/MIPS/RISC V芯片架构



谦川产品

应用场景

智能终端/智能汽车/可信应用管理

智能终端隐私保护场景

唯一符合央行、银联以及国标的TEE方案

智能手机

智能POS终端

车载智能座舱

智能电视

VR终端

Android

vTrust TEE OS

银联云

数字货币DCEP

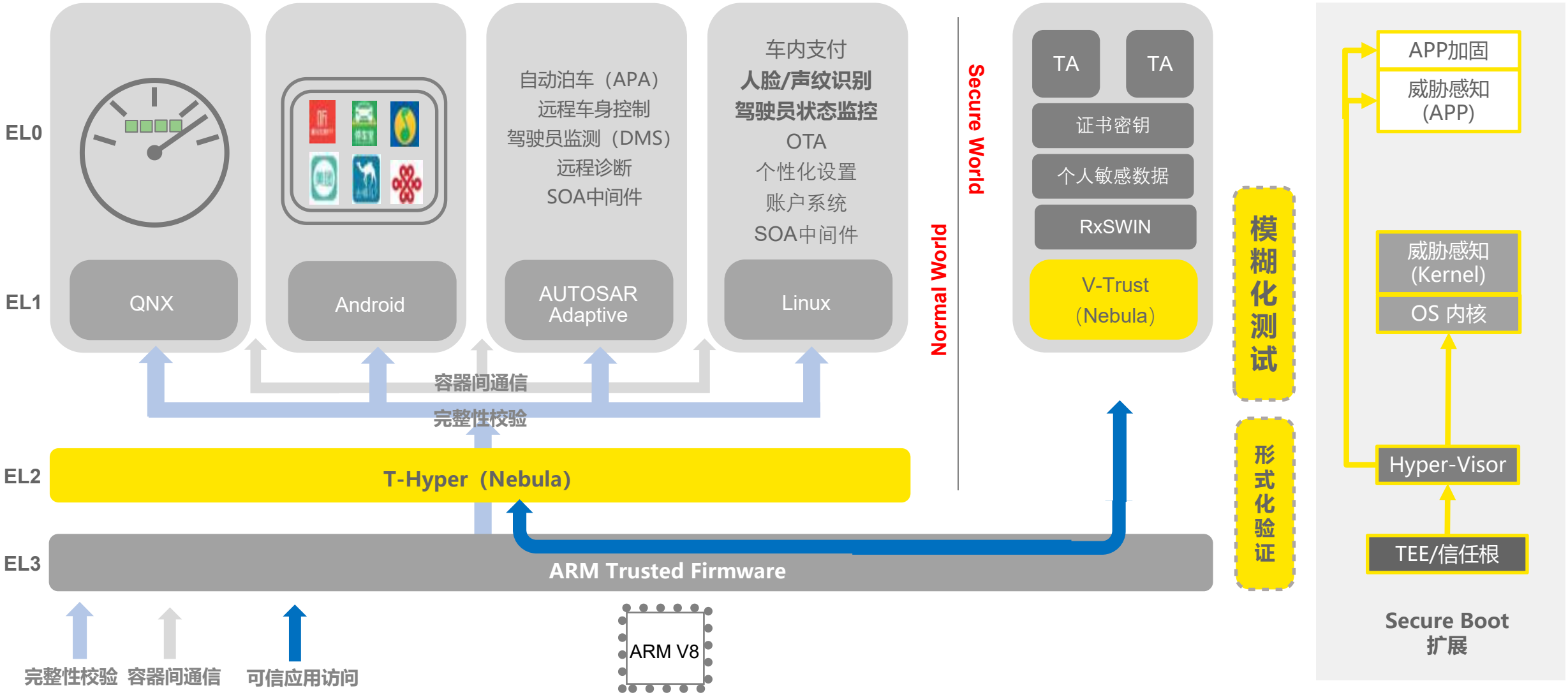
《中国银联支付终端安全技术规范（UPTS 3.0）》

《移动终端支付可信环境技术规范》（JR/T 0156-2017）

《信息安全技术 可信执行环境系统架构规范》

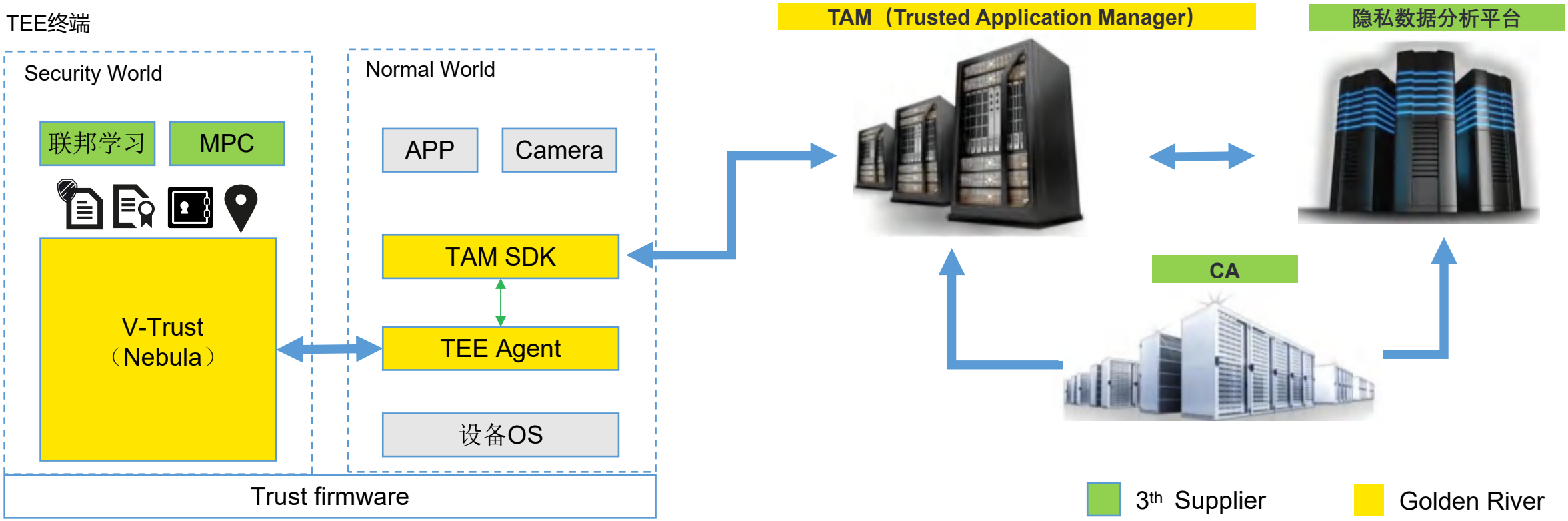
智能汽车隐私保护场景

座舱/智驾/网关等安全集成方案



利用Nebula构架车辆嵌入式安全基座

可信应用管理与双向可信验证




公司介绍

公司介绍
公司概况

1

公司概况

成立于2017年，北京（总部），沈阳（研发子公司）

2

产学研

与清华大学，东北大学深入合作，多项前沿研究成果国际领先，发表多篇国际顶级论文.

3

标准影响力

2011年开始参与中国银联电子支付研究院制定国内第一个TEE可信执行环境规范 —TEEI

2019年受邀参与中国银联电子商务与电子支付国家工程实验室《信息安全可信执行环境技术规范》的TEE国家标准立项工作

4

团队介绍

核心团队由国际顶级安全操作系统专家、芯片级安全工程师、OS内核软件工程师及在校硕士、博士构成。安全微内核 TEE经验平均10年+

.

5

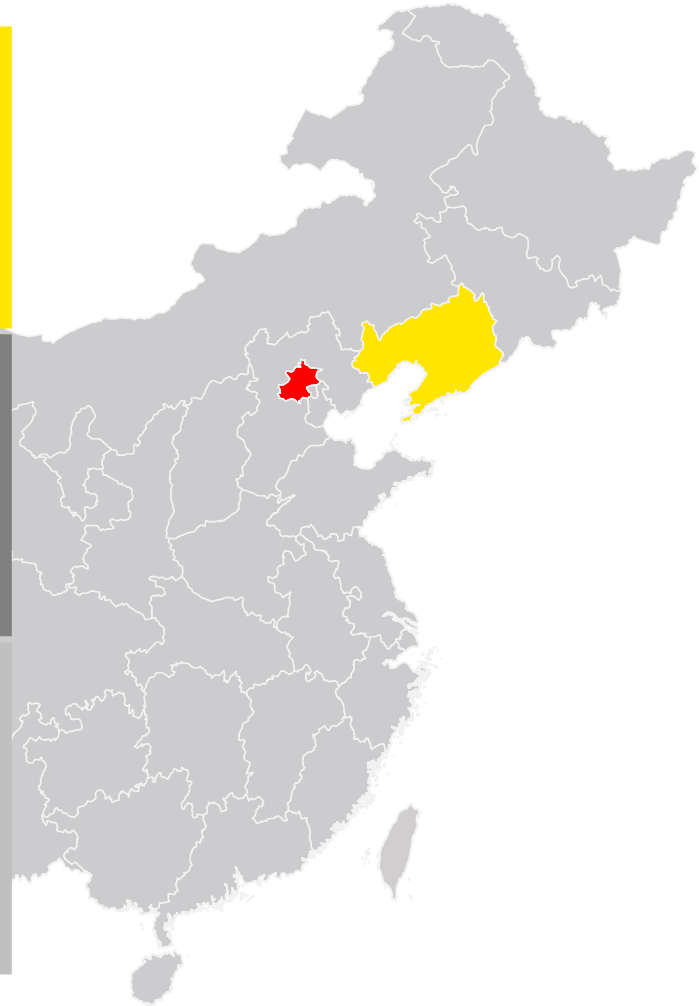
技术能力

可信执行环境，安全微内核，安全虚拟化，形式化验证等多项前沿技术国际领先，国内首创

6

团队执行力

推出了国际上第一个基于安全微内核的全功能TEE产品，该产品曾在国内垄断了90%的第三方TEE市场，在2017年底手机覆盖量预计达到1亿台部署量。2017年立足谦川，面向万物互融新场景，采用了全球最先进的Micro-Hypervisor操作系统架构全新打造了高安全高可靠Nebula微内核，同时支持TEE，HEE，REE三种产品形态。目前，Nebula已经在智能手机，智能POS，物（车）联网领域落地



公司介绍
产学研

1

公司概况

成立于2017年，北京（总部），沈阳（研发子公司），新竹（研发子公司）

2

产学研

与清华大学，东北大学深入合作，多项前沿研究成果国际领先，发表多篇国际顶级论文.

3

标准影响力

2011年开始参与中国银联电子支付研究院制定国内第一个TEE可信执行环境规范 —TEEI

2019年受邀参与中国银联电子商务与电子支付国家工程实验室《信息安全可信执行环境技术规范》的TEE国家标准立项工作

4

团队介绍

核心团队由国际顶级安全操作系统专家、芯片级安全工程师、OS内核软件工程师及在校硕士、博士构成。安全微内核 TEE经验平均10年+

.

5

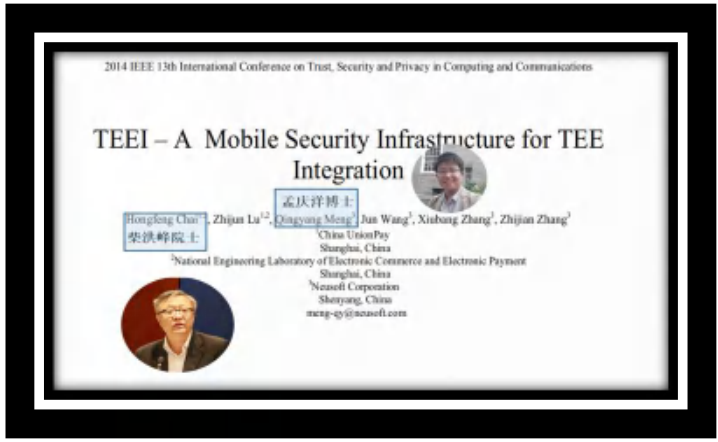
技术能力

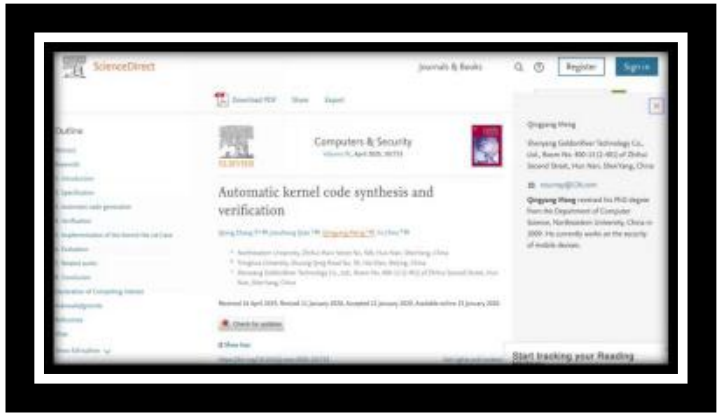
可信执行环境，安全微内核，安全虚拟化，形式化验证等多项前沿技术国际领先，国内首创

6

团队执行力

推出了国际上第一个基于安全微内核的全功能TEE产品，该产品曾在国内垄断了90%的第三方TEE市场，在2017年底手机覆盖量预计达到1亿台部署量。2017年立足谦川，面向万物互融新场景，采用了全球最先进的Micro-Hypervisor操作系统架构全新打造了高安全高可靠Nebula微内核，同时支持TEE，HEE，REE三种产品形态。目前，Nebula已经在智能手机，智能POS，物（车）联网领域落地





公司介绍
标准影响力

1

公司概况

成立于2017年，北京（总部），沈阳（研发子公司），新竹（研发子公司）

2

产学研

与清华大学，东北大学深入合作，多项前沿研究成果国际领先，发表多篇国际顶级论文.

3

标准影响力

2011年开始参与中国银联电子支付研究院制定国内第一个TEE可信执行环境规范 —TEEI

2019年受邀参与中国银联电子商务与电子支付国家工程实验室《信息安全可信执行环境技术规范》的TEE国家标准立项工作

4

团队介绍

核心团队由国际顶级安全操作系统专家、芯片级安全工程师、OS内核软件工程师及在校硕士、博士构成。安全微内核 TEE经验平均10年+

.

5

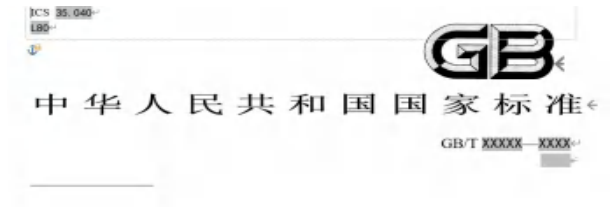
技术能力

可信执行环境，安全微内核，安全虚拟化，形式化验证等多项前沿技术国际领先，国内首创

6

团队执行力

推出了国际上第一个基于安全微内核的全功能TEE产品，该产品曾在国内垄断了90%的第三方TEE市场，在2017年底手机覆盖量预计达到1亿台部署量。2017年立足谦川，面向万物互融新场景，采用了全球最先进的Micro-Hypervisor操作系统架构全新打造了高安全高可靠Nebula微内核，同时支持TEE，HEE，REE三种产品形态。目前，Nebula已经在智能手机，智能POS，物（车）联网领域落地


ICS 35.040
L80

GB

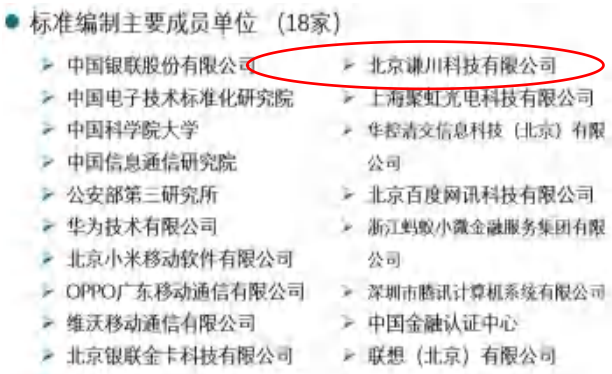
中华人民共和国国家标准

GB/T XXXXX—XXXX


信息安全技术 可信执行环境系统架构

Information Security Technology for Trusted Execution Environment

System Architecture


- 标准编制主要成员单位（18家）
  - 中国银联股份有限公司
  - 中国电子技术标准化研究院
  - 中国科学院大学
  - 中国信息通信研究院
  - 公安部第三研究所
  - 华为技术有限公司
  - 北京小米移动软件有限公司
  - OPPO广东移动通信有限公司
  - 维沃移动通信有限公司
  - 北京银联金卡科技有限公司
  - 北京谦川科技有限公司
  - 上海聚虹光电科技有限公司
  - 华控清交信息科技（北京）有限公司
  - 北京百度网讯科技有限公司
  - 浙江蚂蚁小微金融服务集团有限公司
  - 深圳市腾讯计算机系统有限公司
  - 中国金融认证中心
  - 联想（北京）有限公司

公司介绍
团队介绍

1

公司概况

成立于2017年，北京（总部），沈阳（研发子公司），新竹（研发子公司）

2

产学研

与清华大学，东北大学深入合作，多项前沿研究成果国际领先，发表多篇国际顶级论文.

3

标准影响力

2011年开始参与中国银联电子支付研究院制定国内第一个TEE可信执行环境规范 —TEEI

2019年受邀参与中国银联电子商务与电子支付国家工程实验室《信息安全可信执行环境技术规范》的TEE国家标准立项工作

4

团队介绍

核心团队由国际顶级安全操作系统专家、芯片级安全工程师、OS内核软件工程师及在校硕士、博士构成。安全微内核 TEE经验平均10年+

.

5

技术能力

可信执行环境，安全微内核，安全虚拟化，形式化验证等多项前沿技术国际领先，国内首创

6

团队执行力

推出了国际上第一个基于安全微内核的全功能TEE产品，该产品曾在国内垄断了90%的第三方TEE市场，在2017年底手机覆盖量预计达到1亿台部署量。2017年立足谦川，面向万物互融新场景，采用了全球最先进的Micro-Hypervisor操作系统架构全新打造了高安全高可靠Nebula微内核，同时支持TEE，HEE，REE三种产品形态。目前，Nebula已经在智能手机，智能POS，物（车）联网领域落地

孟庆洋 博士
创始人/董事长/CEO

周博
联合创始人 CTO

郭伟
联合创始人 COO

公司介绍
技术能力

1

公司概况

成立于2017年，北京（总部），沈阳（研发子公司），新竹（研发子公司）

2

产学研

与清华大学，东北大学深入合作，多项前沿研究成果国际领先，发表多篇国际顶级论文.

3

标准影响力

2011年开始参与中国银联电子支付研究院制定国内第一个TEE可信执行环境规范 —TEEI

2019年受邀参与中国银联电子商务与电子支付国家工程实验室《信息安全可信执行环境技术规范》的TEE国家标准立项工作

4

团队介绍

核心团队由国际顶级安全操作系统专家、芯片级安全工程师、OS内核软件工程师及在校硕士、博士构成。安全微内核 TEE经验平均10年+

.

5

技术能力

可信执行环境，安全微内核，安全虚拟化，形式化验证等多项前沿技术国际领先，国内首创

6

团队执行力

推出了国际上第一个基于安全微内核的全功能TEE产品，该产品曾在国内垄断了90%的第三方TEE市场，在2017年底手机覆盖量预计达到1亿台部署量。2017年立足谦川，面向万物互融新场景，采用了全球最先进的Micro-Hypervisor操作系统架构全新打造了高安全高可靠Nebula微内核，同时支持TEE，HEE，REE三种产品形态。目前，Nebula已经在智能手机，智能POS，物（车）联网领域落地

安全微内核技术:

- 对内核及其用户空间驱动与服务采用更加模块化、解耦化设计;
- 建立安全沙箱机制，结合底层芯片安全机制增强堆栈及内存保护机制，精简内核实现，关键逻辑形式化证明，全面提升安全性;
- 建立进程多倍冗余与崩溃重启机制;
- 针对TEE、HEE等芯片隔离环境，研发操作系统新型动态安全多核处理机制及协处理器安全使用机制;

形式化验证技术:

- 采用简单一阶逻辑的数学描述方法替换高阶逻辑;
- 面向专用编译器（如LLVM），采用符号执行技术与一阶逻辑相结合的思路，并通过代码自动生成工具，完成设计描述语言到实现语言的直接翻译;
- 采用模型检测与数学证明相结合的方式，利用当前成熟的开源模型检测框架;

公司介绍
技术能力

1

公司概况

成立于2017年，北京（总部），沈阳（研发子公司），新竹（研发子公司）

2

产学研

与清华大学，东北大学深入合作，多项前沿研究成果国际领先，发表多篇国际顶级论文.

3

标准影响力

2011年开始参与中国银联电子支付研究院制定国内第一个TEE可信执行环境规范 —TEEI

2019年受邀参与中国银联电子商务与电子支付国家工程实验室《信息安全可信执行环境技术规范》的TEE国家标准立项工作

4

团队介绍

核心团队由国际顶级安全操作系统专家、芯片级安全工程师、OS内核软件工程师及在校硕士、博士构成。安全微内核 TEE经验平均10年+

.

5

技术能力

可信执行环境，安全微内核，安全虚拟化，形式化验证等多项前沿技术国际领先，国内首创

6

团队执行力

推出了国际上第一个基于安全微内核的全功能TEE产品，该产品曾在国内垄断了90%的第三方TEE市场，在2017年底手机覆盖量预计达到1亿台部署量。2017年立足谦川，面向万物互融新场景，采用了全球最先进的Micro-Hypervisor操作系统架构全新打造了高安全高可靠Nebula微内核，同时支持TEE，HEE，REE三种产品形态。目前，Nebula已经在智能手机，智能POS，物（车）联网领域落地

硬实时技术:

- 削减操作系统在用户与内核空间的屏蔽中断操作，并设立屏蔽中断时间阈值，优化中断响应时间;
- 减内核TCB及进程栈空间，提升上下文切换速度，并结合底层芯片机制，实现快速上下文切换;
- 基于新型形式化验证方法，对关键操作进行形式化证明，保证执行的确定性;

安全虚拟化技术:

- 充分利用底层HEE芯片隔离技术，增强虚拟机间隔离机制;
- 采用新型被动式虚拟化技术，采用粗粒度页表机制，全面削减嵌入式环境虚拟化带来的开销;

芯片安全隔离技术:

- 在原有TEE芯片隔离技术的基础上，拓展HEE芯片隔离技术，并建立TEE与HEE直接的安全通信机制;
- 面向新型开源RISCV指令集，构建RISCV平台下的TEE解决方案;

公司介绍
团队执行力

1

公司概况

成立于2017年，北京（总部），沈阳（研发子公司）

2

产学研

与清华大学，东北大学深入合作，多项前沿研究成果国际领先，发表多篇国际顶级论文.

3

标准影响力

2011年开始参与中国银联电子支付研究院制定国内第一个TEE可信执行环境规范 —TEEI

2019年受邀参与中国银联电子商务与电子支付国家工程实验室《信息安全可信执行环境技术规范》的TEE国家标准立项工作

4

团队介绍

核心团队由国际顶级安全操作系统专家、芯片级安全工程师、OS内核软件工程师及在校硕士、博士构成。安全微内核 TEE经验平均10年+

.

5

技术能力

可信执行环境，安全微内核，安全虚拟化，形式化验证等多项前沿技术国际领先，国内首创

6

团队执行力

推出了国际上第一个基于安全微内核的全功能TEE产品，该产品曾在国内垄断了90%的第三方TEE市场，在2017年底手机覆盖量预计达到1亿台部署量。2017年立足谦川，面向万物互融新场景，采用了全球最先进的Micro-Hypervisor操作系统架构全新打造了高安全高可靠Nebula微内核，同时支持TEE，HEE，REE三种产品形态。目前，Nebula已经在智能手机，智能POS，物（车）联网领域落地