RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

嵌入式系统的受信任计算 - 不断变化的领域中的挑战

Joerg Borchert
Infineon Technologies

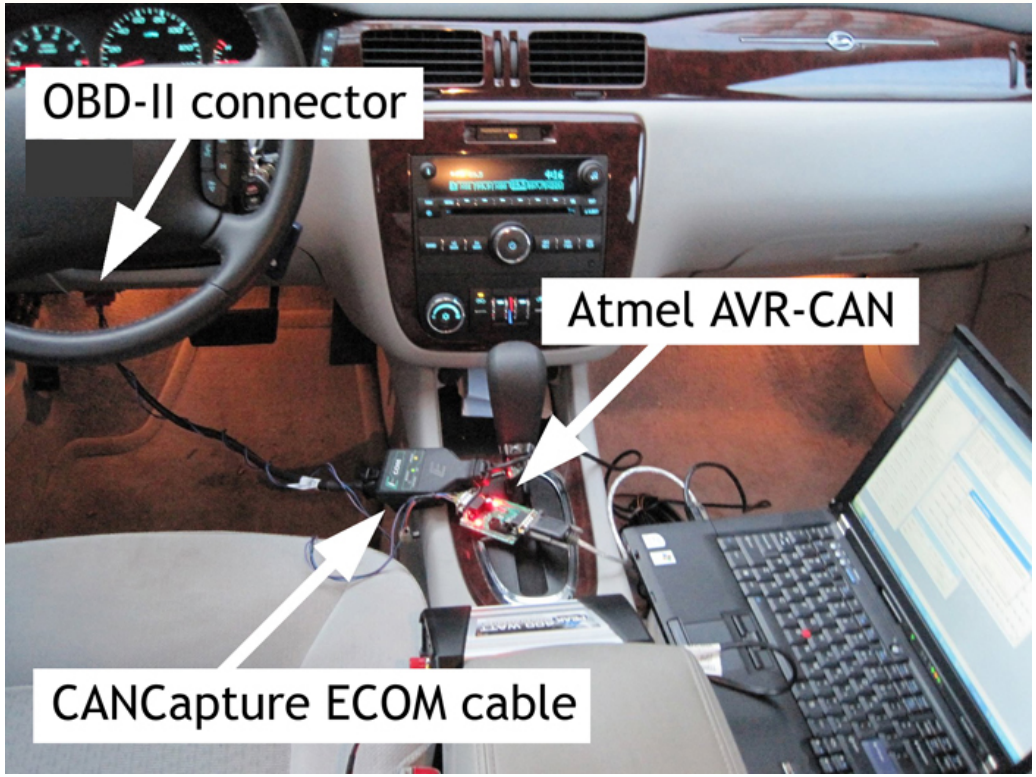
RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

专题会议 ID：TC-2001
专题会议分类：普遍感兴趣

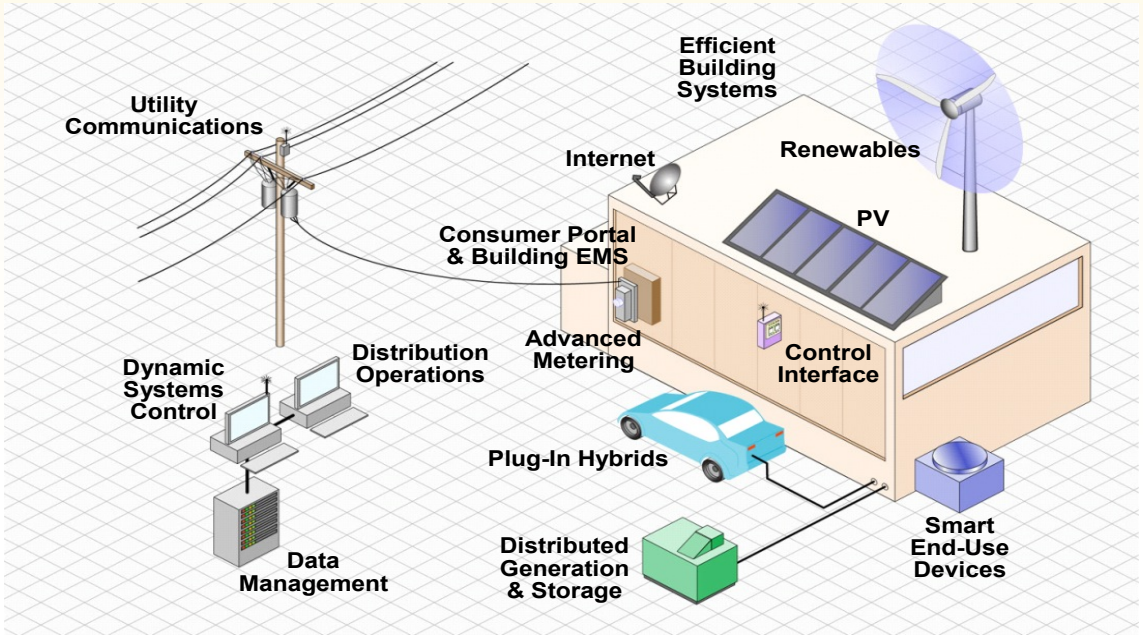
议程

- 日益增多的威胁
  - 嵌入式系统面临风险
  - 来自计算生态系统的经验教训
- 对策
  - 了解攻击
  - 从生物学中学习
- 评估风险

嵌入式系统面临风险：汽车正面临黑客攻击



嵌入式系统面临风险：攻击智能电网



- 威胁来自以下方面：
  - 连接能力、升级能力
  - 成本压力

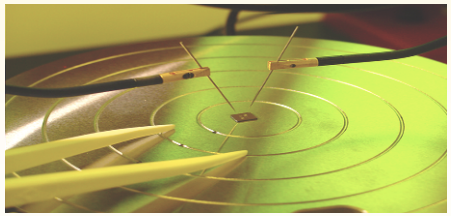
来自 PC 生态系统的经验教训

- 网络中存在不可避免的风险
- 传统防御措施围绕以下方面展开
  - 访问控制
  - 监控流量
- 更高级别的防御体系基于“信任的根源”构建
  - 受信任执行仅发生在安全硬件上（即 TPM）

议程

- 日益增多的威胁
  - 嵌入式系统面临风险
  - 来自计算生态系统的经验教训
- 对策
  - 了解攻击
  - 从生物学中学习
- 评估风险

硬件攻击的 3 种类型

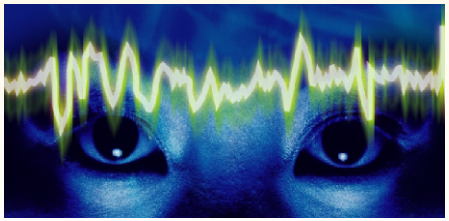


操纵

开发：
几个月

执行：
几天
> 100.000 €

示例：
微区探查



观察

开发：
几天

执行：
几小时
> 10.000 €

示例：
功耗分析

半入侵式

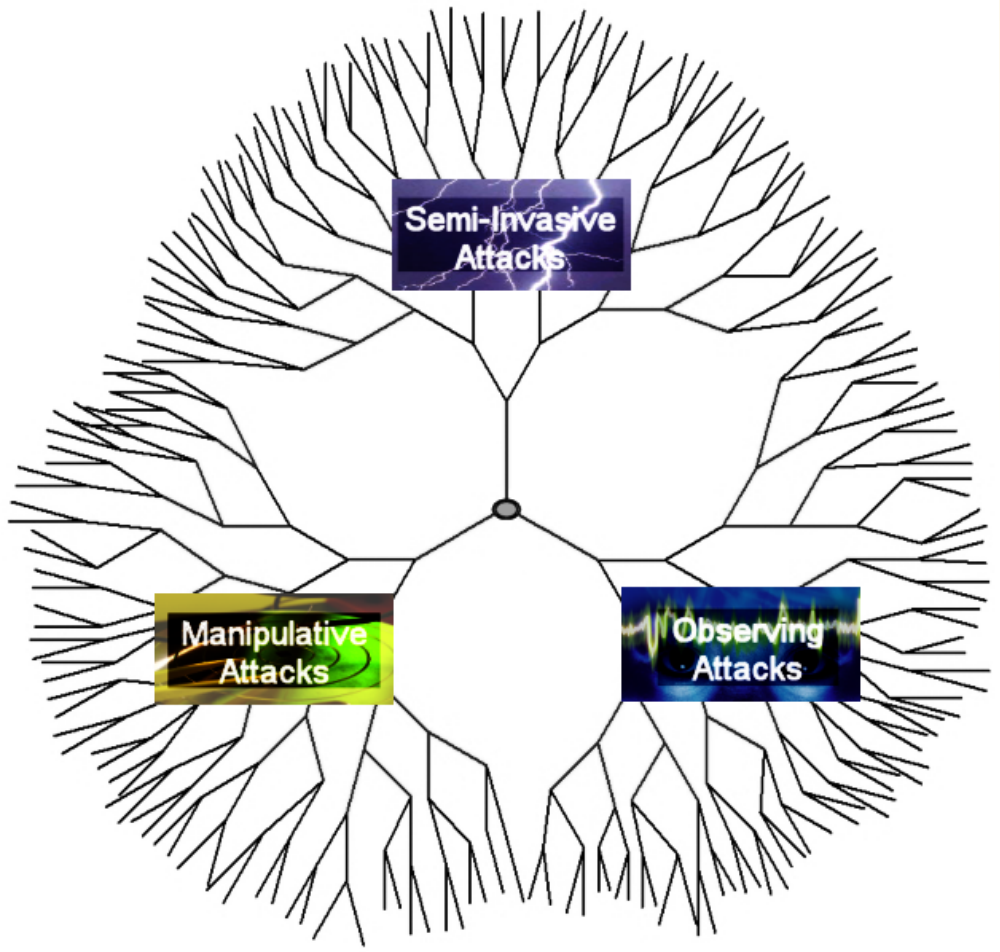
开发：
几个月

执行：
几分钟
> 100 €

示例：
爆发式攻击

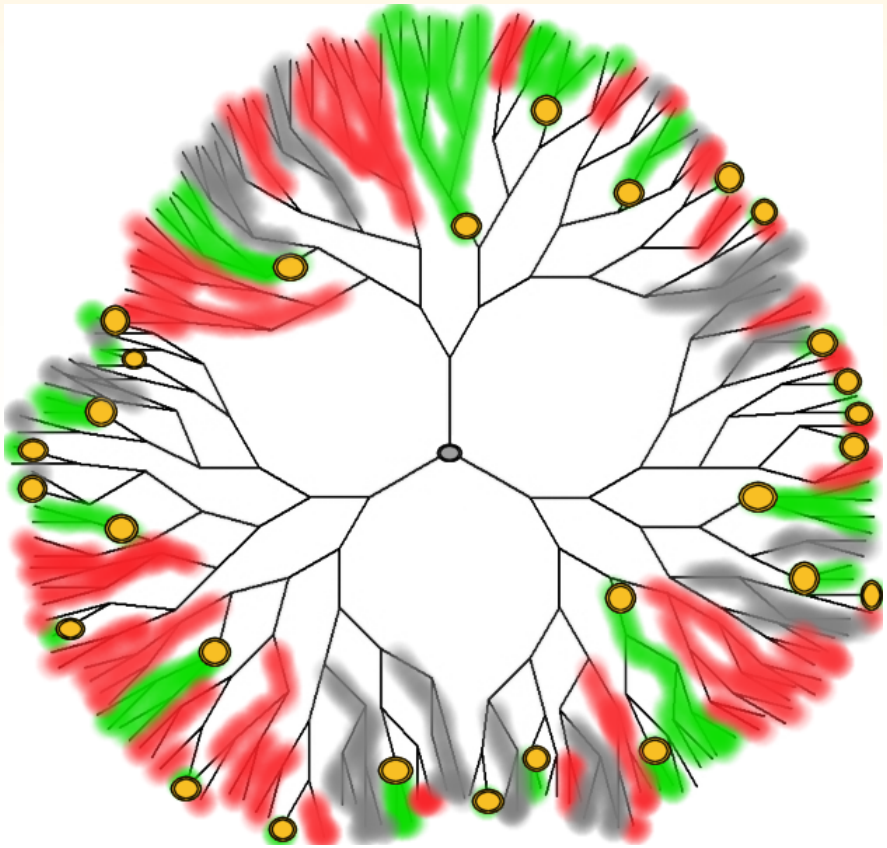
这些类型的攻击需要不同的投资和专业知识。因此，这也将攻击者人群划分为业余攻击者和专业攻击者。

分析攻击类型



- 每种攻击类型都可能产生无限种攻击情形
- 攻击情形在不断地发展演变

传统防御体系：关注攻击情形



对策

受保护

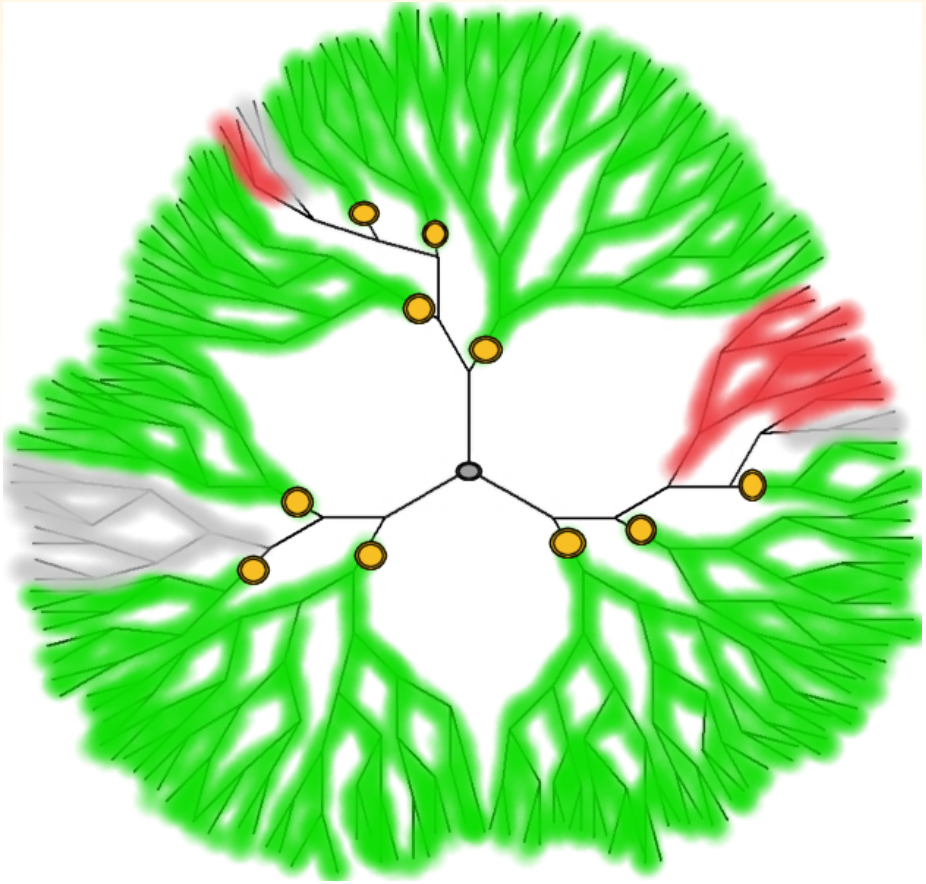
未受保护

未测试，未知

传统对策只能应对一小部分攻击。

需要很多对策，存在许多薄弱环节。

新型防御体系：全面的防御方式



对策

受保护

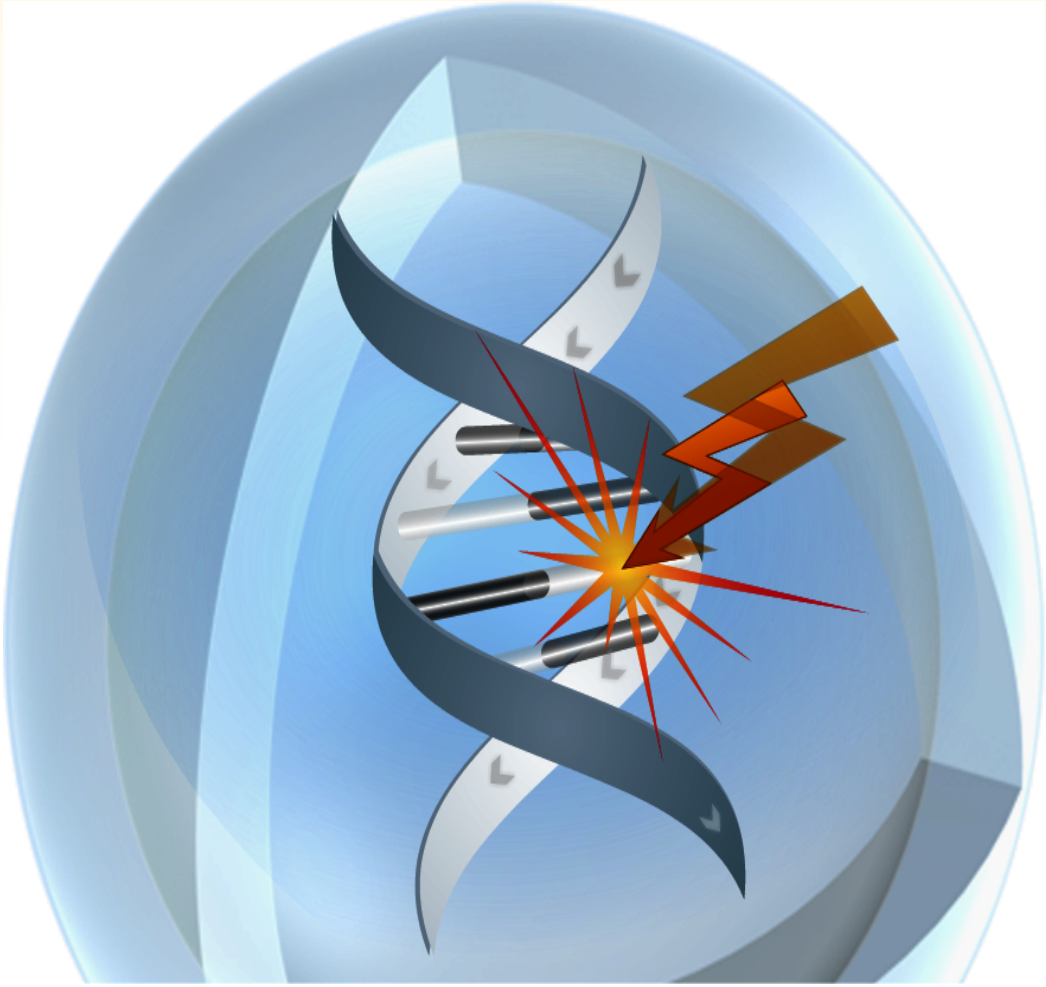
未受保护

未测试，
未知

全面的对策可以防范所有攻击。

需要较少的对策，可以轻松评估风险。

从生物学获得灵感的安全体系



- 细胞就像是安全可靠的计算机，能够完全抵御各种攻击
  - 数据存储和处理受到保护
- 安全 IC 可以效仿自然界法则
  - 自我检查
  - 处理过程完全加密

主要硬件安全概念

- 从模拟模式完全转变为数字安全
- 考虑整个攻击类型，而不是数百万个单独的攻击变体
- 整体安全性得到完善，且不能妨碍功能性
- 依赖效果检测，而不是原因检测
- 安全产品必须坚不可摧
- 安全措施必须易于实施

议程

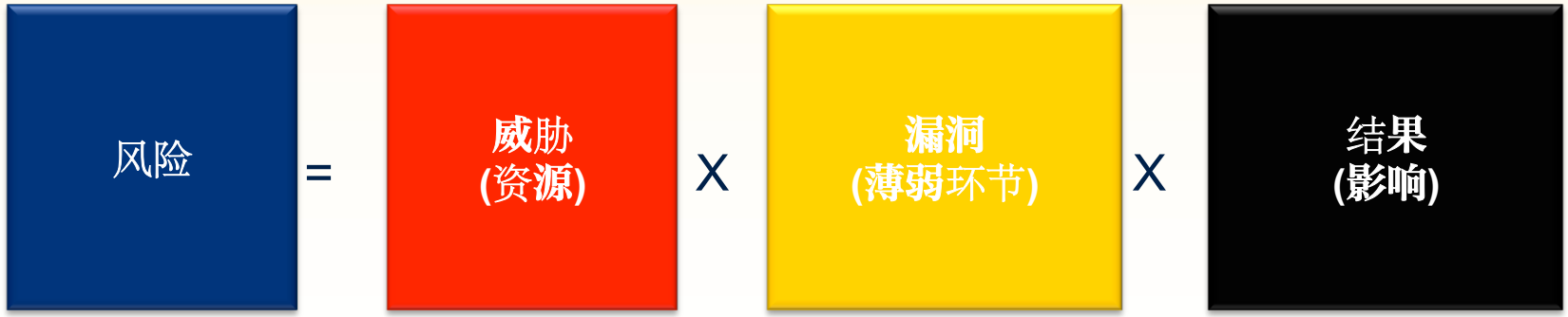
- 日益增多的威胁
  - 嵌入式系统面临风险
  - 来自计算生态系统的经验教训
- 对策
  - 了解攻击
  - 从生物学中学习
- 评估风险

构建防御体系：组织问题

- 成本
- 外包，责任分散
- 设计理念

安全成本：计算

风险分析



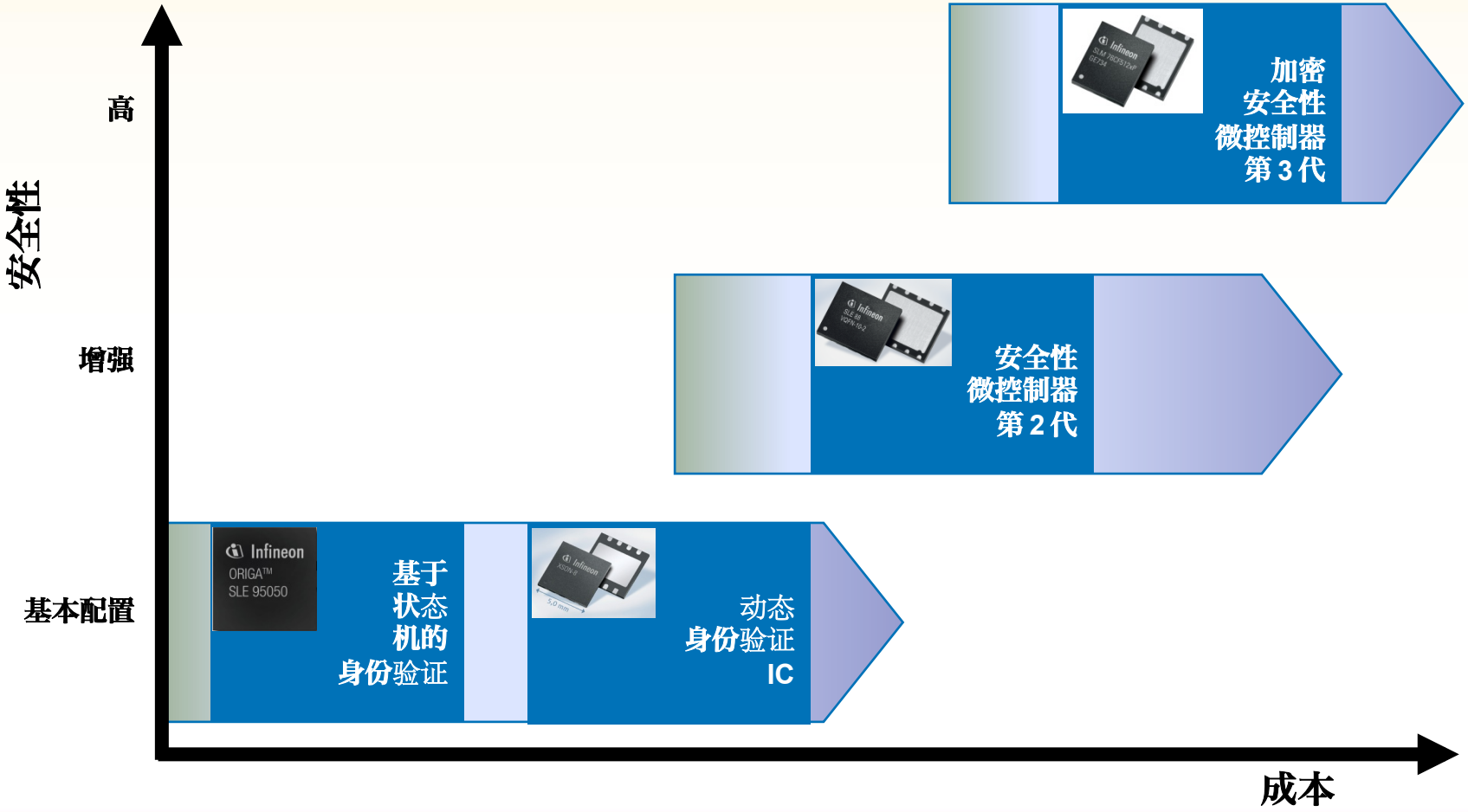
经济性

安全投资相当于买保险

基于风险的选项

- 软件安全
  - 虚拟化
  - 沙盒模型
- 硬件安全
  - 受信任的执行环境
  - 将安全 IC 作为信任的根源

基于硬件的安全性：投资


安全性
高
增强
基本配置
成本
加密
安全性
微控制器
第3代
安全性
微控制器
第2代
Infineon
ORIGA™
SLE 95050
基于
状态
机的
身份验证
动态
身份验证
IC

安全性信任根源

- 安全 IC
  - 确定行为预期
  - 加密是一种方法，但不是唯一的目的
- 验证是信任的基础。 在执行以下操作前进行验证：
  - 发布内存加密密钥
  - 允许在企业网络中使用该密钥
- 安全 IC 使用加密方式来进行验证和识别

标准的作用

- 标准硬件信任根源是成功进行全球部署的基础
  - 全球市场在系统完整性方面将信心倍增

- 可信计算组可提供用于建立国际标准的结构
  - 基于 PC TPM 的工作进行构建可以为嵌入式系统定义硬件安全性

总结

- 嵌入式系统是主要攻击目标
- 可以将受信任计算的原理应用于嵌入式系统
- 对策应针对所有攻击类型，而不仅仅是单个特定攻击情形
- 从模拟安全到数字安全的模式转换是确保长久安全所必需的
- 如今，包含完全加密的数据路径和完全错误检测的安全控制器已经成为信任的根源
- 从经济学角度看，对硬件和软件安全进行投资相当于买保险

谢谢大家！

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012