

智能卡产品“变形记”

未来智能产品安全趋势

刘昕

恩智浦（中国）管理有限公司
2015年 5月 22日



SECURE CONNECTIONS
FOR A SMARTER WORLD

智能卡的演变趋势



智能卡的演进趋势



安全支付 与 安全芯片的未来应用



IOT的安全需求不亚于支付领域的标准

安全只是个借口吗？

網易科技

网易首页 > 网易科技 > IT业界 > 正文

惠普：最热门10款智能家居设备有250个漏洞

2014-08-03 12:59:11 来源: 网易科技报道 有0人参与  分享到 ▼

据科技博客Re/code报道，不少人为前景一片光明的物联网而感到兴奋，黑客们想必亦然。[惠普](#)的一项研究发现，惠普的Fortify应用程序安全部门对市面上最热门的10款消费级物联网产品进行了研究分析，发现它们有250种安全漏洞，也就是说每款产品平均25种。

不过，惠普并没有具体指出涉及哪些产品，只是泛泛地说：它们来自“电视、网络摄像头、家用恒温器、远程电源插座、洒水车控制器、多设备控制中枢器、门锁、家庭警报器、磅秤和车库开门器的制造商”。

这些设备通常都是运行Linux操作系统的精简版本，所以它们会有很多常见于运行Linux的服务器或者计算机的基本安全漏洞。问题在于，设备制造商并没有像对待传统计算机那样花功夫去加强安全保护。

惠普副总裁兼Fortify部门总经理迈克·阿米斯特德（Mike Armistead）指出，该行业的



安全问题的木桶效应

- 犯罪分子总能找到安全上的短板，哪个环节不安全就一定会出问题
- 支付方面的安全问题不仅仅能满足黑客的成就感，更多的是巨大的犯罪收益
- 而物联网的安全出现问题，就造成除了经济损失以外，更大的社会影响

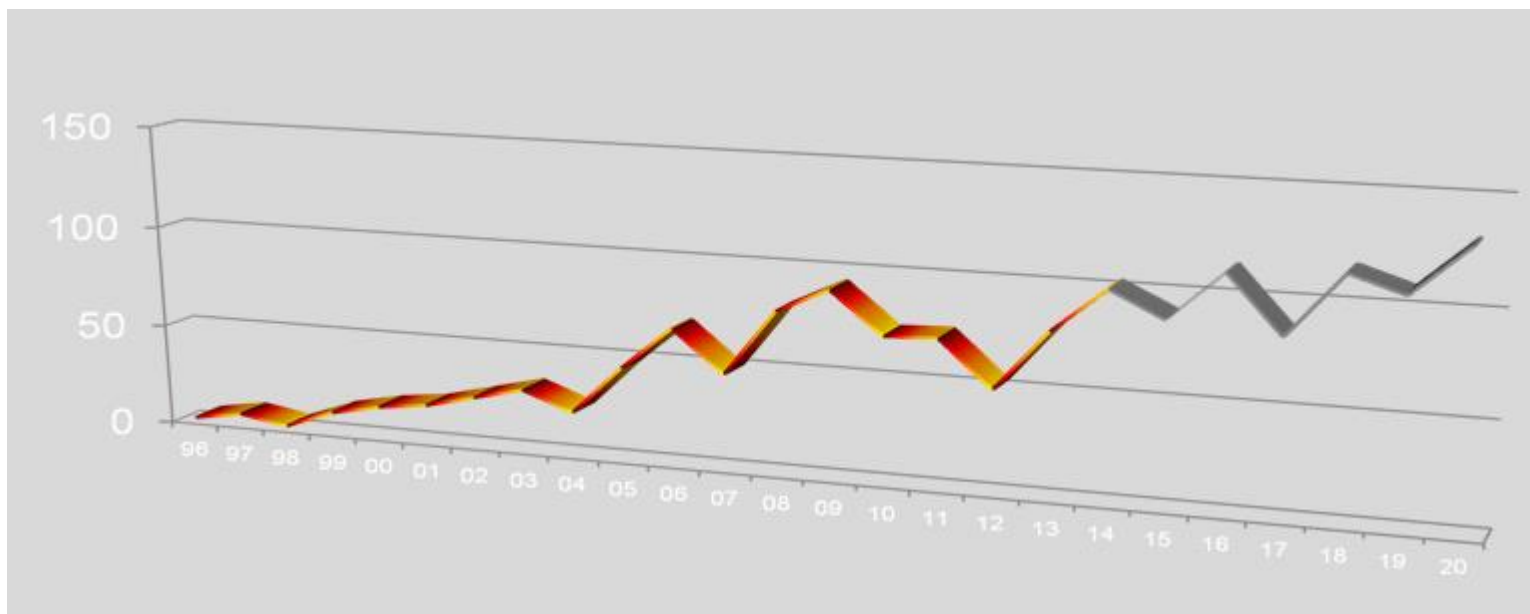


安全芯片攻击趋势



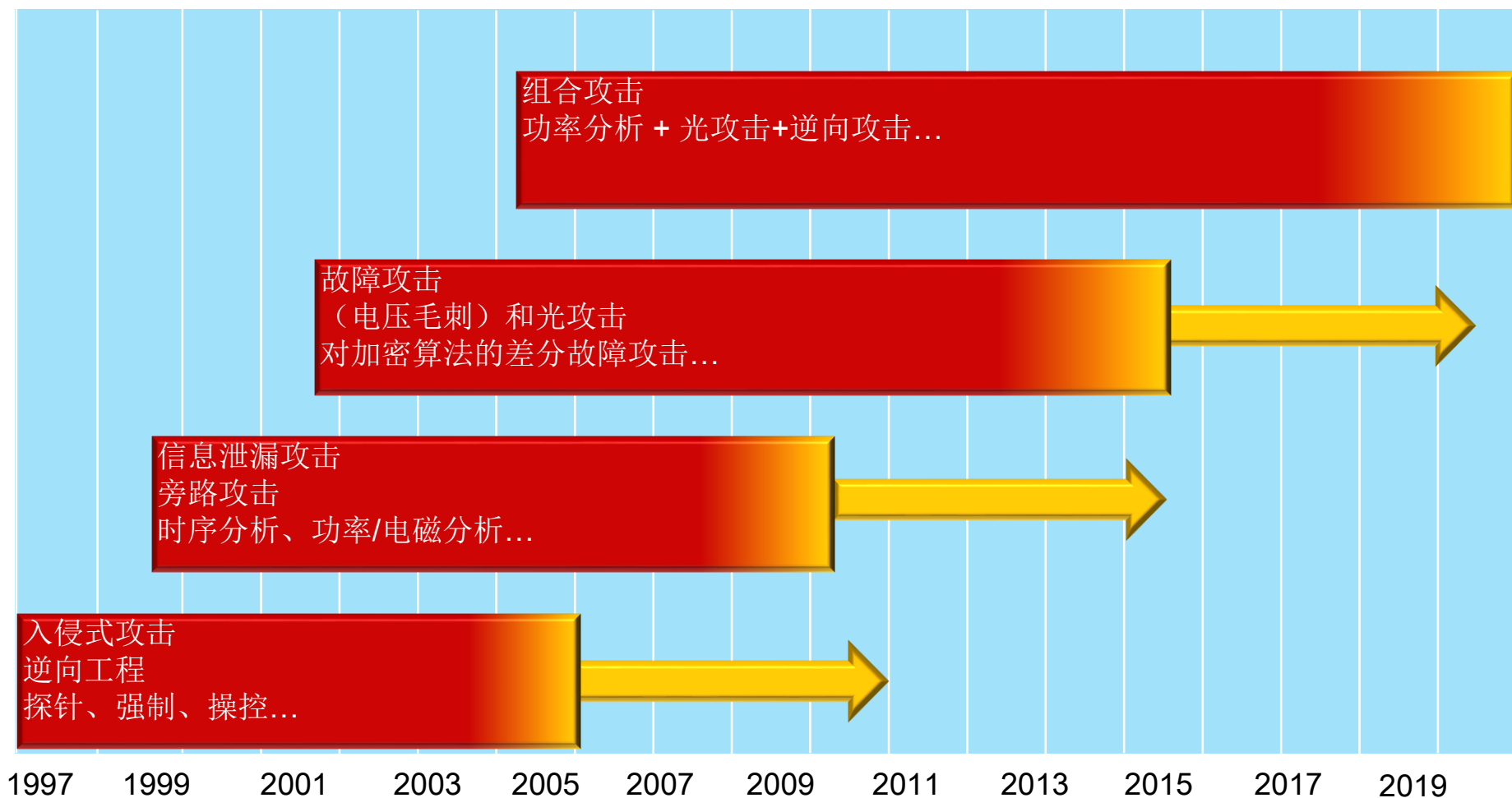
黑客攻击竞赛愈演愈烈

仅嵌入式安全，每年就发表约100篇有关攻击和反制措施的论文。到2014年，论文总数已超过800篇！



产品开发周期需要约2-3年的时间→产品面临风险：如果产品开发过程中对每一个攻击方式的防范措施有疏漏，都会留下产品隐患，并且对下一代的产品也产生影响。

芯片安全防范面临巨大挑战



激光攻击 与 蓝光攻击



INTEGRAL SECURITY™



NXP comprehensive IntegralSecurity™ Concept

More than 100 unique security features harden the SmartMX2

Proven by third party security assessments and type approvals:

CUP security evaluation / BCTC

EMVCo security evaluation

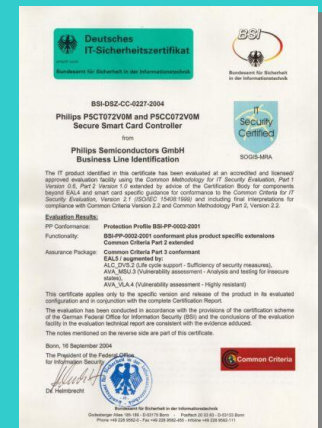
CAST

VISA

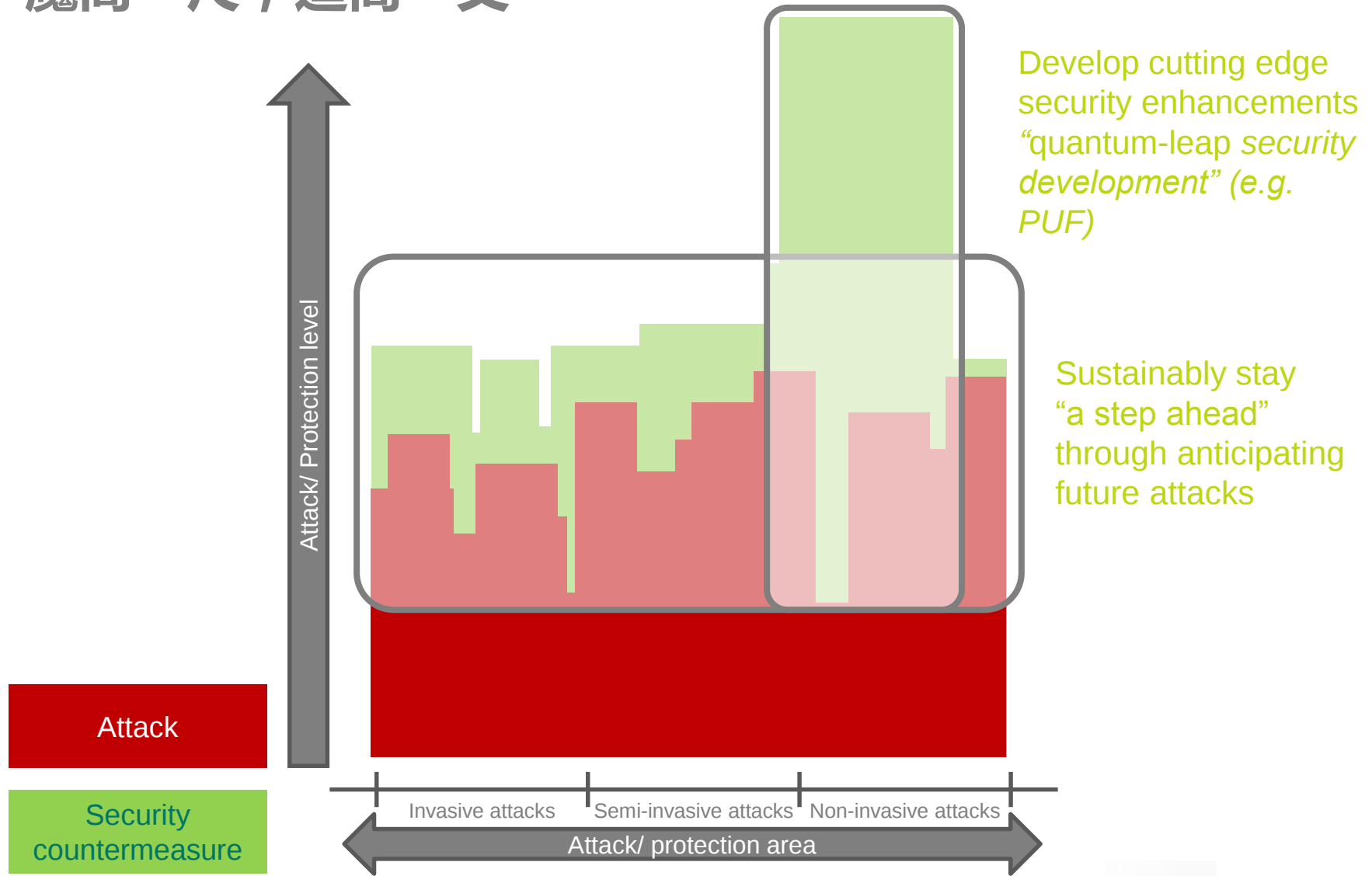
Common Criteria EAL6+

ZKA

Approval for German Signature Card



魔高一尺，道高一丈



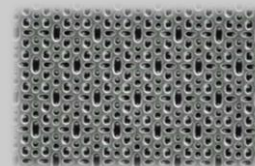
什么是PUF

物理防克隆功能（PUF）——IC芯片的指纹

PUF

本质性

Random pattern (“0” and “1” bits)
generated by embedded SRAM cells



唯一性

Each IC has it's own pattern determined
by manufacturing process generates



稳定性

Random pattern persist over the whole life cycle



IC芯片的指纹

物理防克隆功能（PUF）——提升安全性与可验证性



安全性

- Keys not stored in NVM → No read out possible
- Keys only available during decryption window → Diminish the attack time



可验证性

- Authentication of the IC
 - Counterfeit protection
 - Life time authentication
 - Clone protection

IC芯片的指纹

安全无止境

- 没有最安全，只有更安全
- 安全领域里的博弈永远不会休止
- 任何对安全的放松都会导致灾难性后果





SECURE CONNECTIONS
FOR A SMARTER WORLD