万物互联
从安全产品走向产品安全

演讲人：谭晓生

职务： 360 副总裁

日期： 2014年9月25日

万物互联的后移动互联网时代

- Google收购Nest
- Apple推出iWatch
- Jawbone
- 小米路由器
- Tesla电动车
- 能上网的电冰箱
- 智能医疗设备
- ……

万物皆成为黑客破解的对象

- 2014Defcon上黑客演示45分钟破解22种硬件设备
- SyScan360上黑客破解Tesla电动车
- 2013年家用路由器被黑风波
- USB Firmware被重写的问题

什么安全产品可以解决问题？

- 防火墙？
- IPS？
- IDS？
- UTM？
- VPN？
- SOC？
- 扫描器？

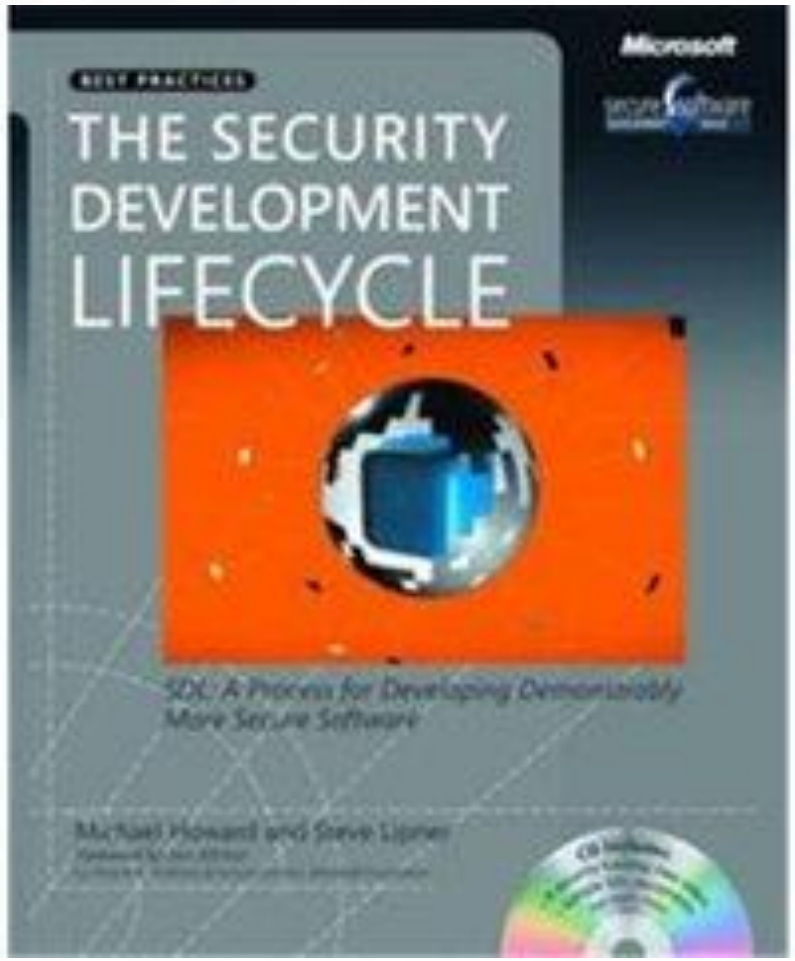
回到问题的原点

- 脆弱性是如何引入的？
- 脆弱性是否可以完全消除?
- 如何减小脆弱性造成的影响？

可供借鉴的历史—漏洞披露

- 国家信息安全测评中心
- 乌云漏洞报告平台
- 360库带计划

可供借鉴的历史



- 软件的脆弱性是如何改进的？
  - 安全开发周期，即Security Development Lifecycle (SDL)
- Web安全的脆弱性是如何改进的？

电路板调试模式的问题

- 硬件设计中常见的调试接口有：
  - JTAG接口
    - » 单片机烧写以及Debug调试接口
  - TTL串口
    - » 单片机通用的数据交互接口
  - USB接口
    - » 单片机嵌入式系统新兴的高速数据交互接口

这些调试接口的存在，一是方便设计开发，而是方便故障分析，但现在大多数硬件厂商，并未对这些接口进行安全方面的加固。

Firmware被篡改的问题

- 硬件设备的Firmware
  - Firmware可以是单片机的程序固件
    - » 比如飞思卡尔、pic等等常见的单片机，使用jtag或者别的接口将程序固件写入。
  - Firmware也可以是EEPROM或者FLASH
    - » 比如常见的嵌入式系统，系统和程序放在外置的存储芯片当中。
  - Firmware可以被篡改
    - » 可以通过硬件固有的烧写接口，比如JTAG、SPI、I2C等接口直接对单片机或者存储芯片进行烧写
    - » 也可以通过软件调试交互接口，比如串口，比如USB，在数据交互过程中，对原数据进行修改。

无线通信协议脆弱性问题

- 2014 BlackHat多个软件无线电安全议题
  - 黑客拥有了多种的无线电协议分析利器
    - » HackRF、BladeRF、DVB-T电视棒等廉价设备
    - » 黑客出色的协议分析能力得已延展到物联网通信领域
    - » 可监听、截获任意无线电频率的通信报文
    - » 可发出、伪造任意无线电频率的通信报文
  - 大量物联网节点、智能家居产品依赖无线通信
    - » WiFi、ZigBee、RF
    - » 2.4Ghz、315/433/868/915Mhz
  - 产品研发人员缺乏应有的安全意识
    - » 通信协议未采取加密认证或采取的加密强度不高
    - » 安全意识不足研发的无线设备会遭到无线黑客的痛击

安全公司的角色

- 产品安全开发流程
- 产品安全解决方案
- 产品安全开发顾问咨询服务
- 产品安全评测服务
- 云安全中心运营

政府的角色

- 制定国家标准
- 产品的市场准入控制
- 科研课题的设置
- 对产品安全事故追责的法律法规

智能硬件制造企业的角色

- 将产品安全纳入产品设计流程管理
- 承担有安全缺陷产品的赔偿责任
- 对有安全缺陷的产品实施召回

Thanks!