

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



China Internet Security Conference 2014
2014中国互联网络安全大会

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被重写的問題



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



WooYun.org 已关注 10.7万

首页 厂商列表 白帽子 团队 漏洞列表 提交漏洞 安全中心 企业招聘 知识库 公告

当前位置: WooYun >> 首页 WooYun的rank系统设置, 漏洞评价将影响最终rank

最新提交 (55)

提交日期	漏洞名称	评论/关注	作者
2014-09-18	龙背网旗下消费网SQL注入一枚	0/0	路人甲
2014-09-18	一个SQL注入可致广电总局内网渗透	9/14	niliu
2014-09-18	万POA 无限制多参数sql注入	1/2	路人甲
2014-09-18	espcms sql注入漏洞	1/2	Noxxx
2014-09-18	某航空公司多个业务系统漏洞命令	4/2	路人甲
2014-09-18	一种进入某航空公司多套服务器的漏洞	3/12	路人甲

最新确认 (771)

提交日期	漏洞名称	评论/关注	作者
2014-09-16	阿里旗下淘宝网某系统后台漏洞命令	0/2	路人甲
2014-09-18	小米VPN账号密码登录可登录	2/12	吴友仁
2014-09-18	小米内网漫游记(一个漏洞命令导致各种内部系统瘫痪)	33/101	临工
2014-09-18	小米内网漫游记(漏洞披露)	2/16	野子
2014-09-13	联通某重要开放平台命令执行	0/3	花猪猪
2014-09-13	某系统调用漏洞引发的蝴蝶效应之可以获取河南某市大量人口身份信息	16/37	路人甲

最新公开 (20768)

提交日期	漏洞名称	评论/关注	作者
2014-09-18	腾讯手机管家对加推木马造成无礼	0/1	壹轮舞
2014-09-13	主券商利用XSS+STRUCT2任意执行命令	1/6	姜秀不...

360 漏洞计划 漏洞列表 提交漏洞 白帽排行 库带社区 申诉列表 库带超市 登录 注册

9月12日打靶名单: 点这! 小米厂商漏洞奖励升级: 点这!

第三方漏洞收集平台

安全 公正 可信赖

我要提交漏洞

限制获取任意数据(带头大猪), 估价 ¥3000 2014-09-16, CmsEasy漏洞SQL注入漏洞可获取管理员账号等信息(带头大猪), 估价 ¥3000 2014-09-16

最新安全事件	最新漏洞	已付赏漏洞	平台动态
8088...	某市多个银行网站存在SQL注入漏洞		2014-09-17
360漏洞奖励2014年9月第二次发放日程			2014-09-15
今日漏洞打靶情况, 恭喜三位! (2014.9.12)			2014-09-12
关于小米厂商漏洞奖励计划开始实施 (2014.9.10)			2014-09-10
关于360漏洞奖励计划开始实施的公告			2014-09-09

漏洞奖励升级方案

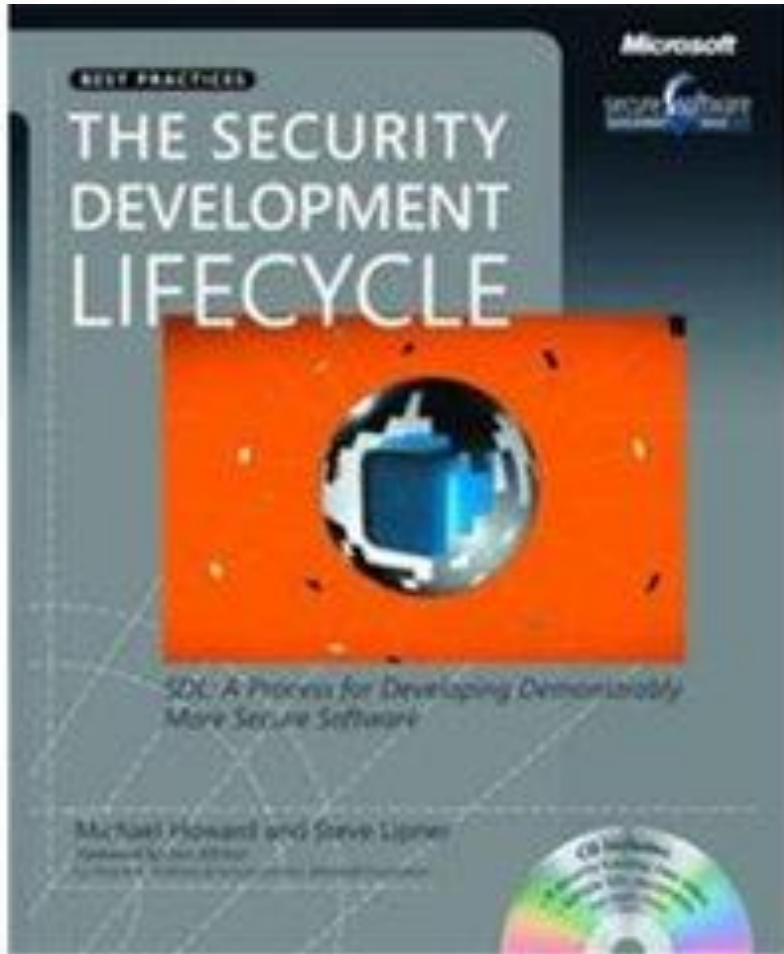
这里聚集了各类代码审计大神、漏洞挖掘大神, 我们希望通过安全奖励机制激励白帽们挖掘并发现此类高危漏洞的漏洞, 解决拥有几十万、上百万甚至上千万的网站用户系统的安全问题。来, 我们一起去搞点牛逼的事情! [点击查看更多>>](#)

ABOUT US / 关于我们

作为国内最权威的网络安全厂商, 我们组建了网站站长、白帽子、第三方建站程序厂商, 以大家共同利益为出发点, 本着公正、可信的原则, 向整个互联网

- 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!