

新型媒体建设中的信息安全管控

演讲人：谭晓生

职务：奇虎360 副总裁，首席隐私官

日期：2015年6月17日

媒体被黑客攻击事件



攻击的目标

- 个人计算机
 - 个人移动终端（手机、平板电脑、电子阅读器）
 - 服务器
 - 工业控制系统/嵌入式系统
 - 物联网传感器/智能机器
 - 网络设备/信息传输装置
 - 云计算系统
- 

为什么这些目标会被攻破？

- 计算机体系结构的天然缺陷
- 网络通信协议的缺陷
- 管理制度的缺陷
- 人的缺陷

系统漏洞现状

终端 办公系统	操作系统	Windows XP、Windows Vista、Windows7、Windows8、IOS 等
	应用系统	Office、WPS、Acrobat、浏览器、即时通讯工具、下载工具、播放器 图片处理工具、邮箱客户端、在线炒股客户端、在线游戏客户端等
	BYOD	iPhone、iPad、HTC、三星、Nokia、Microsoft 等
业务 支撑系统	操作系统	Windows Server 2003、Windows Server 2008、WinCE AIX、HP-UNIX、Solaris、FreeBSD、Linux系列
	应用系统	Oracle、SQL Server、Web Logic、ERP、BPM、OA 工业控制系统、其他业务软硬件系统
网络 基础设施	网络设备	交换路由设备、网络运维设备、网络安全设备
	Wifi	AP、AC

▶▶ 每年会发现数千个0DAY漏洞

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2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被重写的的问题

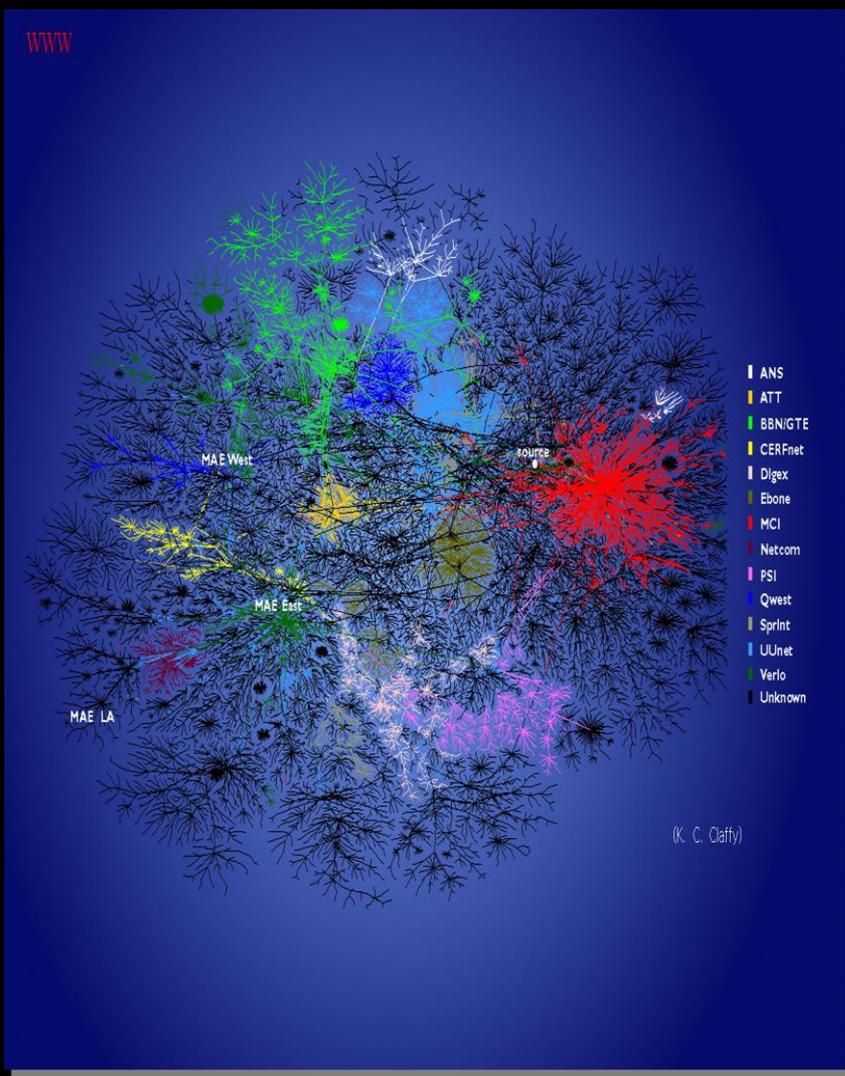


传统的意识：安全即边界

- 防火墙
- IPS
- IDS
- UTM
- VPN
-



传统的意识：安全即边界



- 互联网的本质是什么？
- 云计算对网络边界的冲击
- 移动应用对网络边界的影响
- 智能硬件对网络边界的影响
- 现在的世界是一个无边界网络
- 随着网络的泛化和无边界化
- 边界思想越来越不适应整个网络发展的现状

企业信息安全边界在哪里？

- 企业网站
- 企业Wifi
- BYOD
- 智能硬件设备
- 供应链
- 互联网路由
-



安全体系的演化

早期的P2DR安全模型



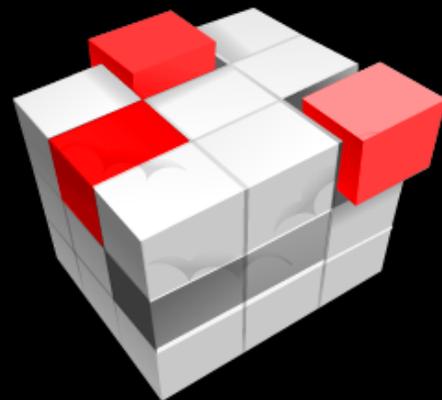
本质：安全就是响应+防护的安全运维体系

后来的安全木桶理论



本质：安全就是用安全产品堆砌出来的线式防御体系

流行的立体防御体系



本质：安全就是分层的、分级的多层次防护体系

安全——4个重要假设

如何发现有漏洞被利用/攻击行为检测？

系统有未发现的漏洞

找出哪些漏洞还没有修补，进行修补

系统有已发现的漏洞未修补

如何发现系统已经被渗透了？
清理
如何重现攻击过程？
如何溯源？

系统已经被渗透

如何发现员工的异常行为？
如何检测/拦截来自内网的攻击？

员工不可靠

安全理念：三个阵地

- 产品
- 对外服务
- 员工

- 重要服务器
- 重要业务系统
- 重要数据

- 监控
- 审计
- 大数据分析

争夺边境线

保卫大城市

反潜伏

第一道防线

第二道防线

第三道防线

新安全模型：云+管+端

云端

- 攻击行为学习
- 攻击模型提取
- 漏洞检测
- 攻击行为鉴定

终端

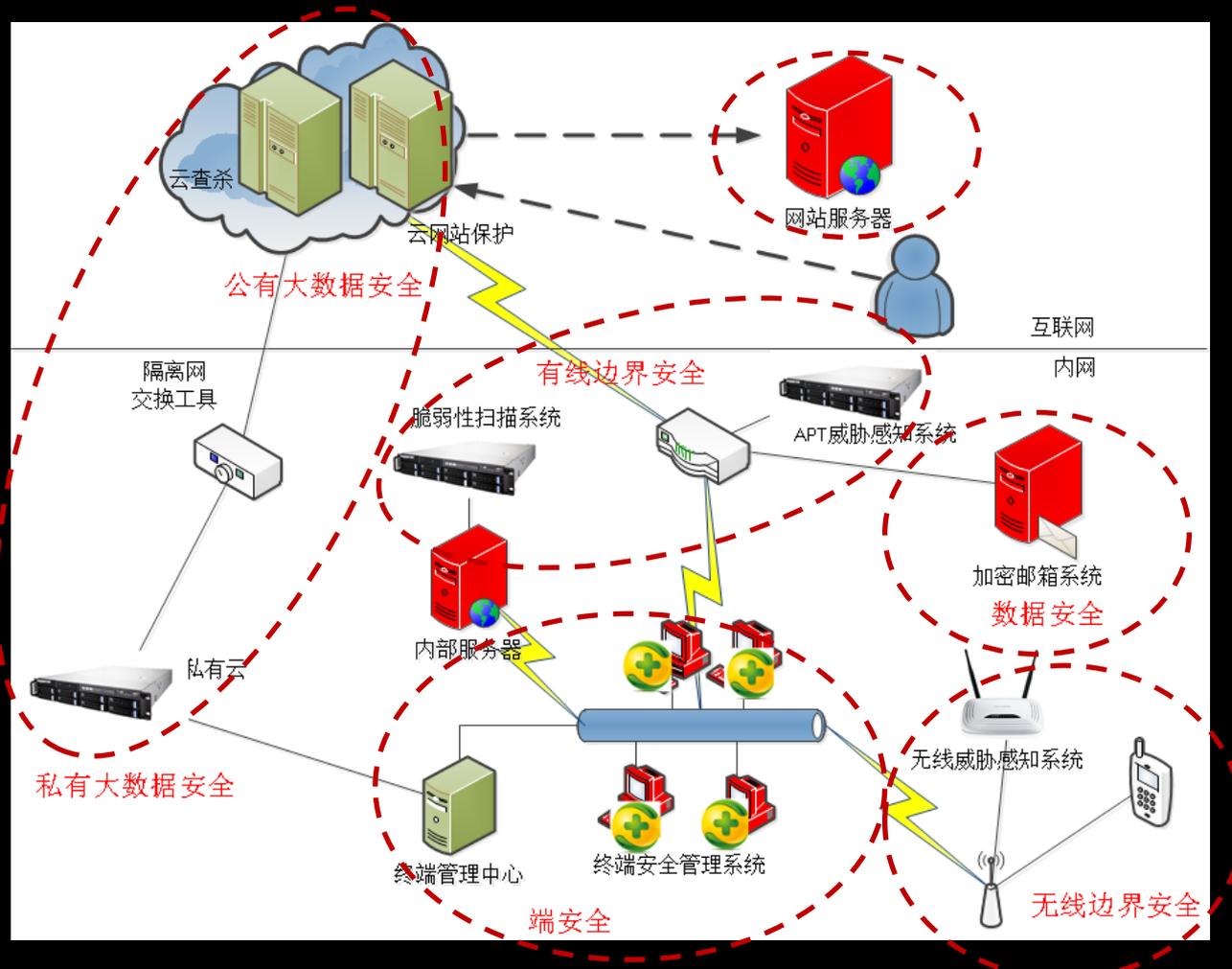
- 统一管控
- 多维信息提取
- 软件准入
非白即黑
- 主动防御

管道

- 网关防护
- 准入控制
- 流量侦听



新的安全边界在哪里？



新的安全边界在哪里？

- 端
 - PC机
 - 手机
 - 智能终端
- 网络（边界、管道）
 - 出口路由器
 - 核心交换机
 - 各种网络安全设备
- 云计算基础架构

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

WooYun.org 10.7万

WooYun.org Frank机制改进, 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	走秀网旗下购物网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	万户OA 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弱口令	4/2	路人甲
2014-09-18	一种进入某航空公司多台服务器的姿势	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	阿里旗下海淘网某系统后台弱口令	0/2	路人甲
2014-09-18	小米VPN账号密码泄露证实可登录	2/12	吴衣仁
2014-09-18	小米内网漫游记(一个弱口令导致各种内部系统泄露)	33/101	临时工
2014-09-18	小米内部员工邮箱泄露	2/16	胖子
2014-09-13	联通某重要开放平台命令执行	0/3	花花酱
2014-09-13	某系统通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	腾讯手机管家对加壳木马查杀无力	0/1	瘦瘦胖
2014-09-13	走秀网利用XSS+STRUCT2任意执行命令	1/6	姿势不...

360 库带计划

第三方漏洞收集平台
安全 公正 可信赖

我要提交漏洞

9月12日打款名单: 点这! 小众厂商奖励策略升级: 点这!

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

新安全事件	新通用漏洞	已付款漏洞	平台动态
360库带超市2014年9月第二次发货日期	来自多个政府网站台式SQL注入漏洞		2014-09-17
今日库带打款情况, 恭喜土豪们! (2014.9.12)			2014-09-15
关于小众厂商系统的漏洞奖励计划开始实施 (2014.9.10)			2014-09-12
关于360库带超市商品兑换与发货的公告			2014-09-10
			2014-09-09

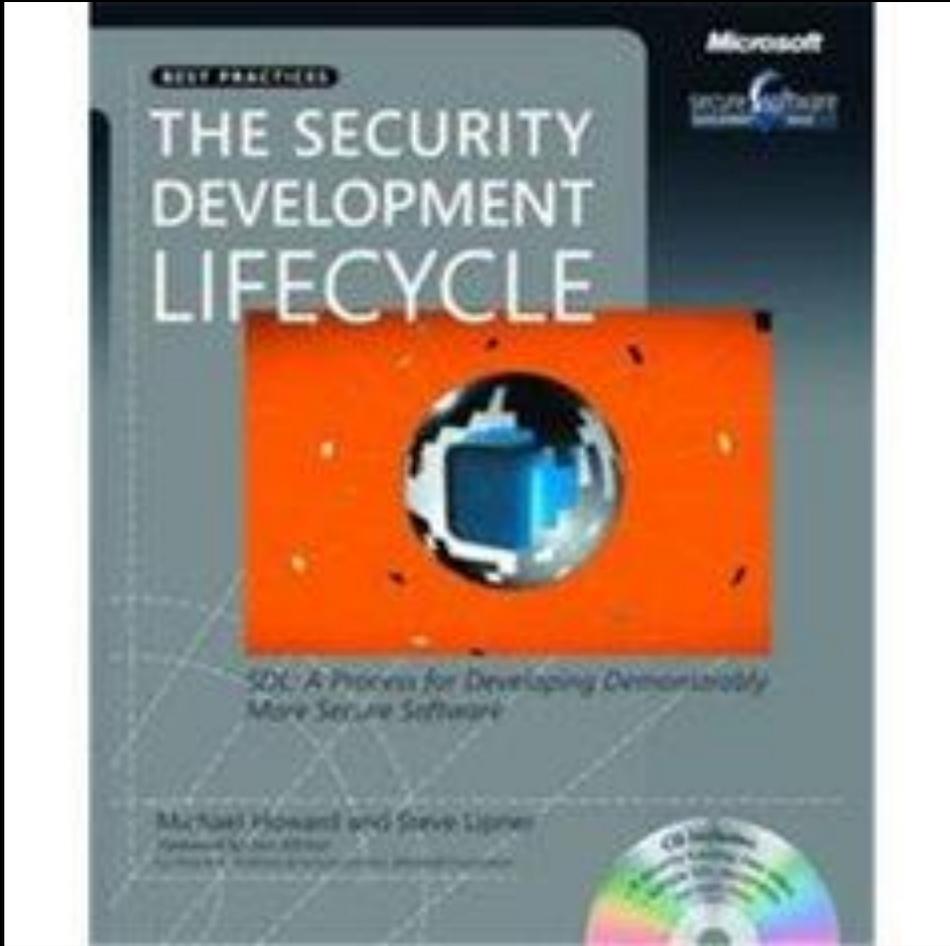
漏洞奖励升级方案

这里聚集了各类代码审计大牛、漏洞挖掘大拿, 我们希望通过高奖金奖励机制激励白帽们挖掘并发现此类重点应用的漏洞, 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, 我们一起做点牛逼的事情! 点击查看更多>>>

ABOUT US / 关于我们

作为国内最权威的网站安全厂商, 我们聘请了网站站长, 白帽子, 第三方建站程序厂商, 以大家共同的利益为出发点, 本着公正、可信的原则, 向整个互联网证

可供借鉴的历史



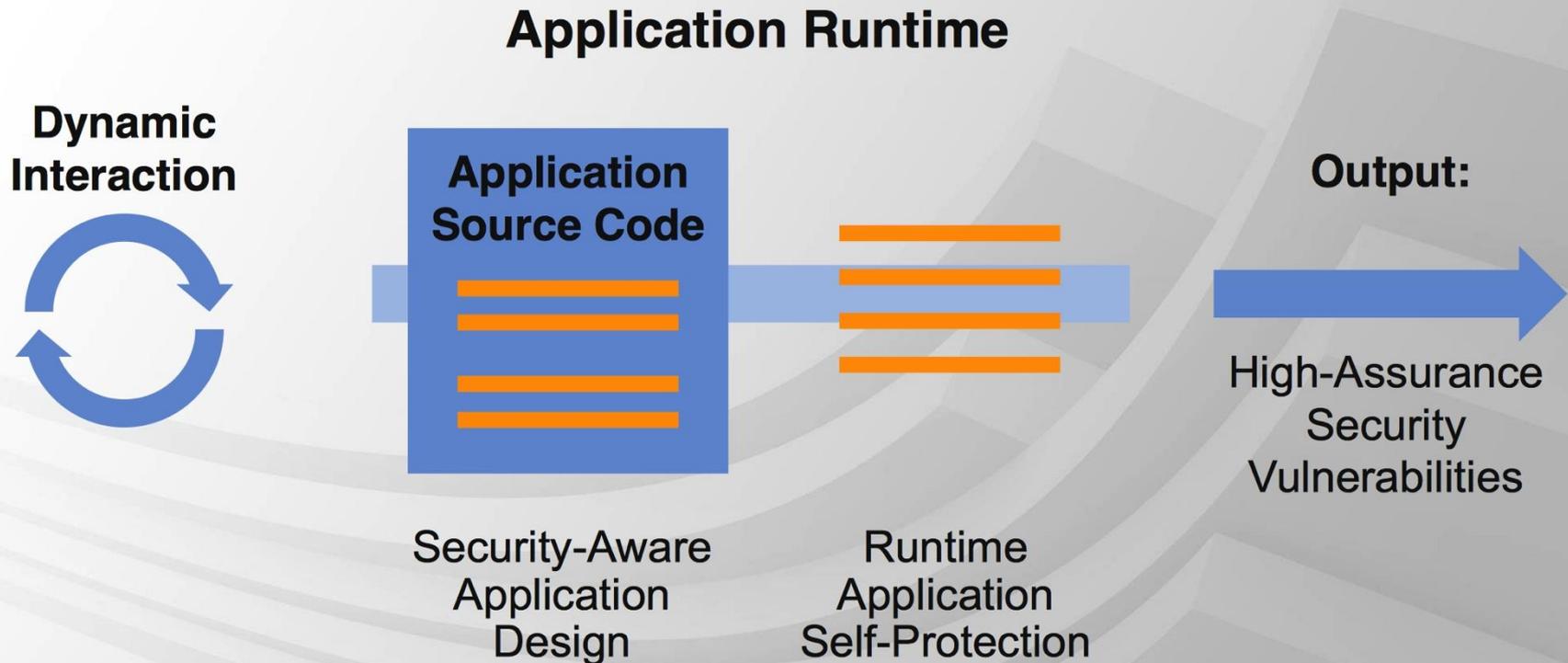
软件的脆弱性是如何改进的？

- 安全开发周期，即Security Development Lifecycle (SDL)

Web安全的脆弱性是如何改进的？

系统应该可以自我保护

Enable Applications to Protect Themselves



Thanks!

