测试为网络安全保驾护航

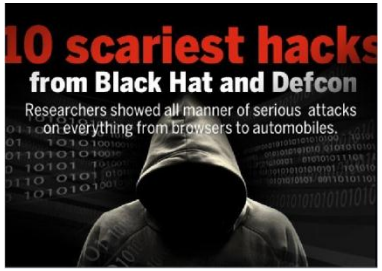
演讲人：张小东

职务：思博伦通信中国区技术总监

日期：2014年9月24日

网络安全现状

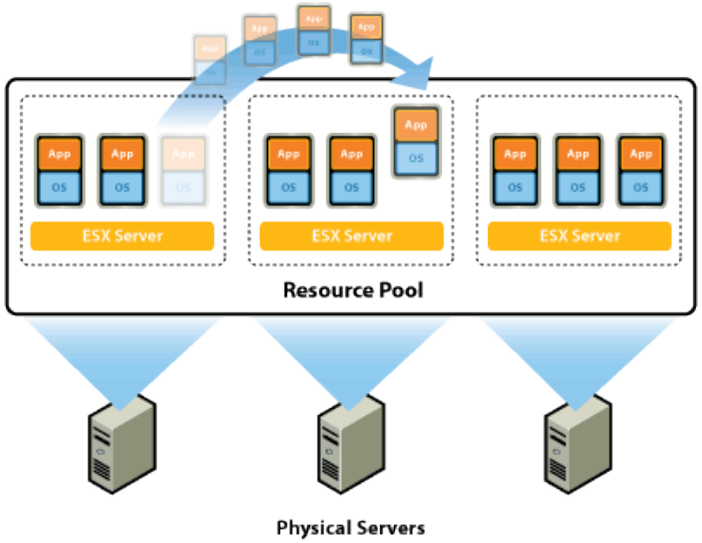
- 恶意软件（病毒、蠕虫、木马、宏病毒、垃圾邮件、间谍软件、广告软件、Rootkit、记键程序，等等），Botnet、网络入侵、DDoS攻击、网络钓鱼、数据窃取， …



- 针对新互联网应用的新变种（社交网络）
- http://www.f-secure.com/weblog/archives/00001517.html (Facebook)
- http://thenextweb.com/twitter/2013/04/22/criminals-hijack-twitter-accounts-using-malware-that-injects-javascript-code-to-send-malicious-tweets/ (Twitter)

技术和市场趋势


BYOD
Bring Your Own Device

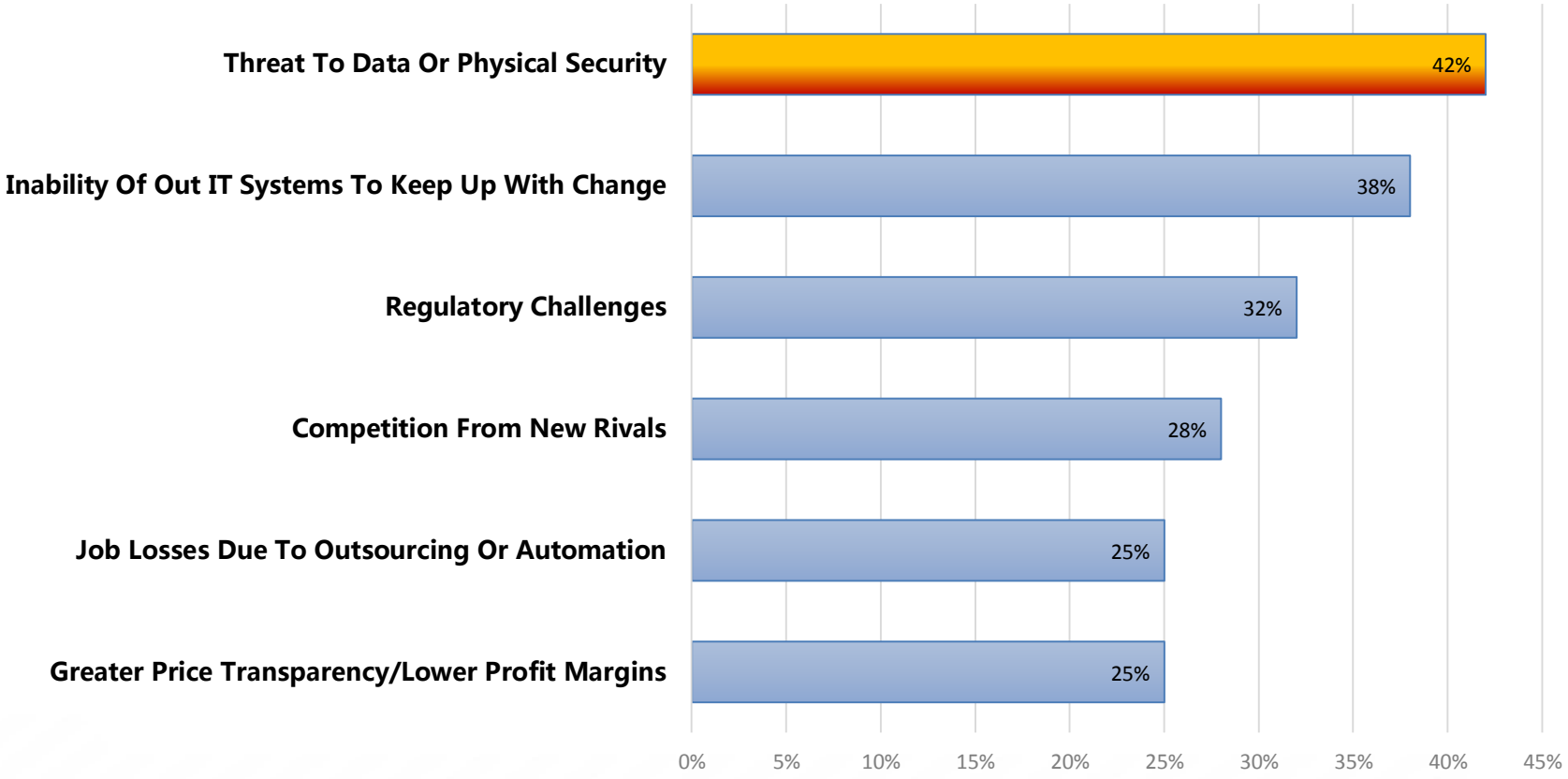

App
OS
ESX Server
Resource Pool
Physical Servers


hulu
Gmail
YAHOO! Mail
skype
flickr
FARM VILLE
PANDORA
amazon video


v1.1.1

网络安全是首要因素

万物互联的潜在影响



Source: Cisco, n=7000+ global executives

Business Insider

测试对于网络安全的重要性

- 如何保证网络或设备的性能和安全性？
- 如何平衡性能和安全性？
- 如何保证正确处理最新的应用/内容？
- 如何保证网络或设备在处理真实流量时，保持性能和安全性？

防火墙测试标准发展

- 防火墙测试标准
  - 基准测试标准RFC 3511
  - 针对RFC 3511标准的缺陷，各重点实验室对RFC 3511进行补充
- 防火墙测试内容和趋势
  - 指标测试应用现网流量统计模型，从采用真实报文内容，到更真实的报文大小，到单连接多事务处理数量
  - 单指标测试向指标集成测试（新建、并发、带宽指标互为背景测试）
  - 基于HTTP的测试向多种业务综合测试，HTTP+FTP+MAIL+...
  - 针对防火墙增值能力的扩展或者下一代防火墙的发展，对于各类应用的DPI能力测试
  - IPSec能力测试
  - 防火墙抗攻击，攻击流量识别，健壮性测试

思博伦是防火墙测试国际标准主要制定者

Network Working Group
Request for Comments: 3511
Category: Informational

B. Hickman
Spirent Communications
D. Newman
Network Test
S. Tadjudin
Spirent Communications
T. Martin
GVNW Consulting Inc
April 2003

Benchmarking Methodology for Firewall Performance

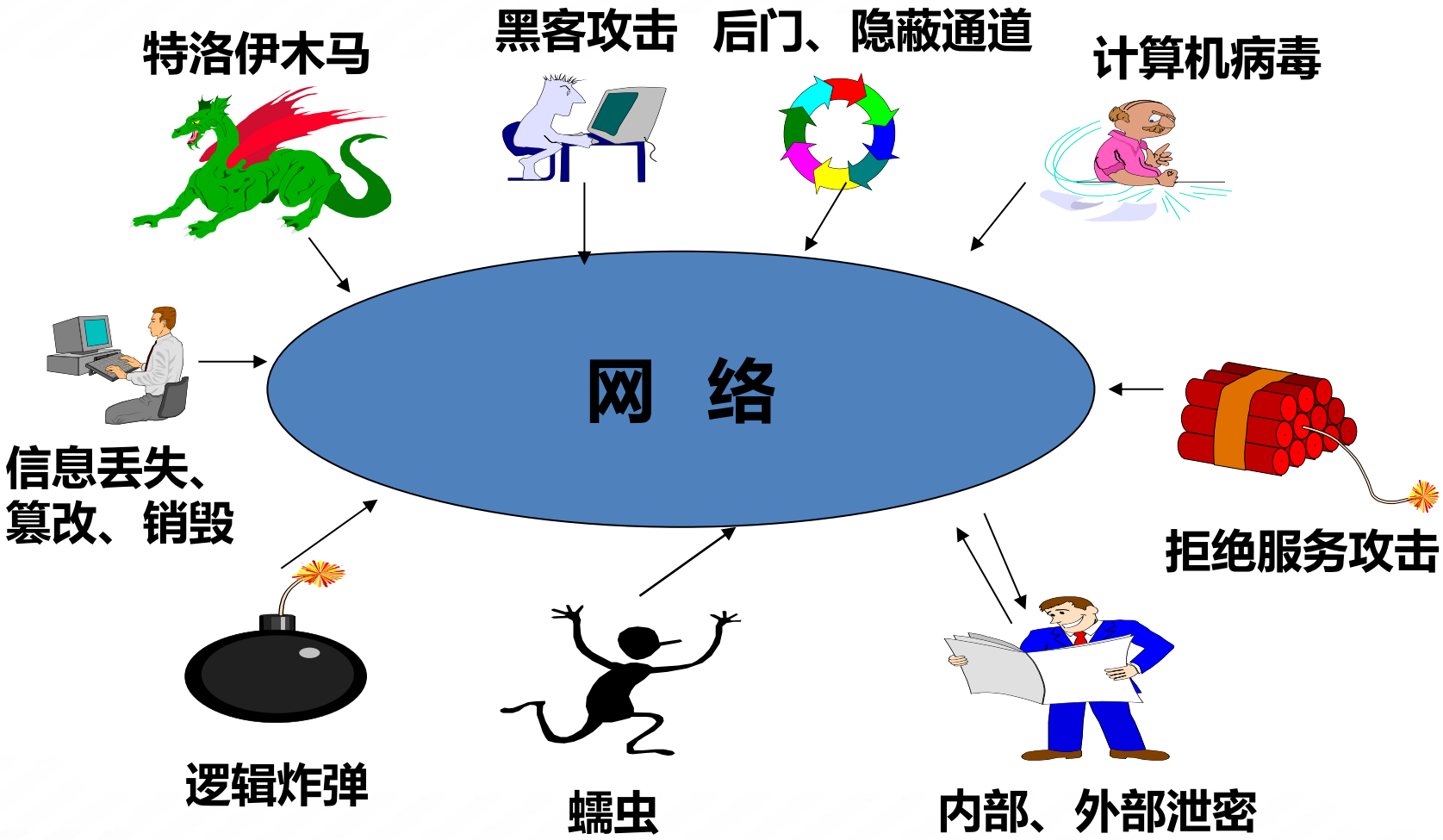
Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

防火墙测试新条目

测试条目	测试目标	Layer
并发测试（以新建为背景）	测试用户并发容量。 验证20%新建速率是否影响并发容量，验证条件： • 工作在NAT模式 • 测试内容为512K以上，真实录制的现网网页内容，如“新浪” • 验证重叠、乱序包能正确处理	L4-7
新建测试（以并发为背景）	测试新建速率性能 验证20%并发用户背景是否影响用户新建速率，验证条件同上。	L4-7
有效流量（混合新建、并发）	根据现网统计模型，构造并发，新建和有效流量并存的测试	L4L7
多种应用流量模型测试	测试防火墙在一定规则条件下，对多种应用流量混合流量的处理能力，比如HTTP：FTP：MAIL=7：2：1	L4L7
IPSEC测试	测试防火墙IPSEC容量，IPSEC新建速率，IPSEC流量	L3L7
新应用识别能力	对启用DPI功能的网元，测试应用识别能力	L4L7

网络中存在的安全威胁

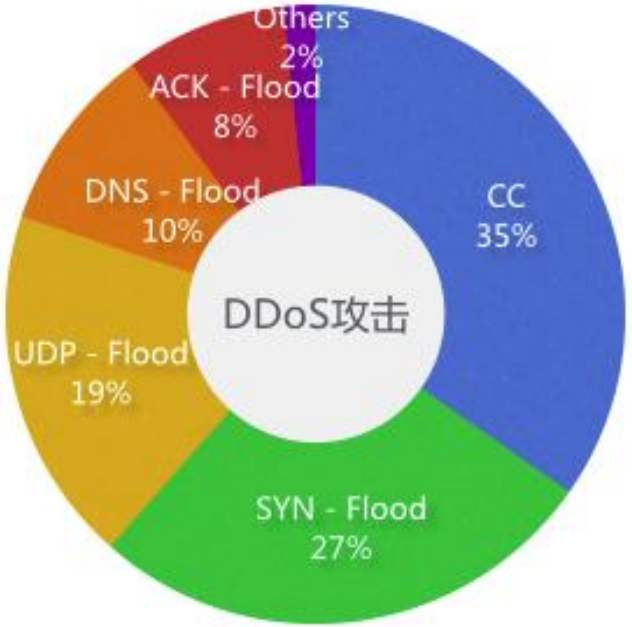


分布式拒绝服务攻击 DDoS

- DDoS是利用网络上已被攻陷的电脑作为“僵尸”，向某一特定目标电脑发动密集式的“拒绝服务”式攻击，用以把目标电脑的网络资源及系统资源耗尽，使之无法向正常请求的用户提供服务。
- 最早发现于1998年，但在现网攻击中样本中，会发现很多活跃的DDoS。
- 传统DDoS攻击可以分成两种形式：带宽消耗型以及资源消耗型。它们都是通过大量合法或伪造的请求占用大量网络以及设备资源，以达到瘫痪网络及系统的目的。
- 新兴DDoS在不同层面进行带宽消耗和资源消耗：如Apapche Killer、Slowloris消耗HTTP服务器的相应能力，针对云主机则消耗CPU处理资源，可用带宽，达到超过SLA限额而主动下线效果。
- 最新的DDoS攻击流量已经达到400Gbps规模。

DDoS种类举例

- ARP Flood
- Evasive UDP
- Land
- Ping of Death
- Ping Sweep
- Random Unreachable Host
- Reset Flood
- Smurf
- Syn Flood
- TCP Port Scan
- Teardrop
- UDP Flood
- UDP Port Scan
- DNS Flood
- Unreachable Host
- Xmas Tree
- TCP FIN Flood
- TCP SYN Flood
- TCP AYN/ACK Flood
- SIP Flood
- HTTP Flood（CC）
- Windows XP UDP Flood DoS
- IPv6 Fragment Flood
- Slowloris

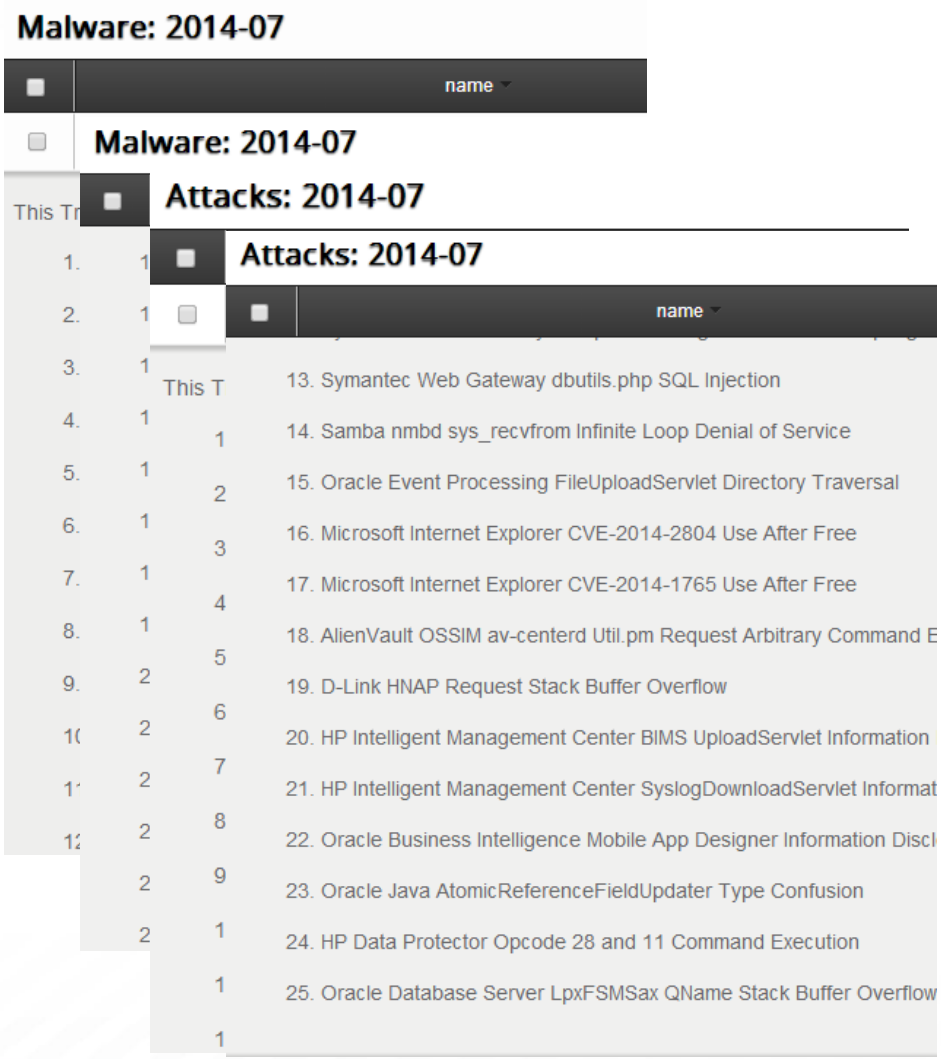


DDoS仿真测试

- DDoS功能和流量测试
  - 源自长期安全研究积累
  - 开放接口，用户可以自行构造添加新的DDoS攻击
  - 多种流量模型（Ramp、Burst、Random、pulse）
  - 检测正常业务是否被阻断
- DDoS 和正常流量混合
  - 混合DDoS 流量和正常流量
  - 衡量正常流量用户体验，衡量DDoS流量阻断效果
  - 测试设备CPU占用率和队列深度
- 内嵌攻击
  - 用特有的动作列表和模拟用户技术来模拟中间人攻击
  - 在IPSec和SSL-VPN通道上产生攻击

公开漏洞测试方法

- 支持8000多种攻击手法
- 攻击库每月更新
- 攻击模型包含了多种软件平台和攻击场景
- 混合攻击流量和业务背景流量使用同一个端口发送
- 同时测试恶意攻击识别能力和系统的正常业务处理能力



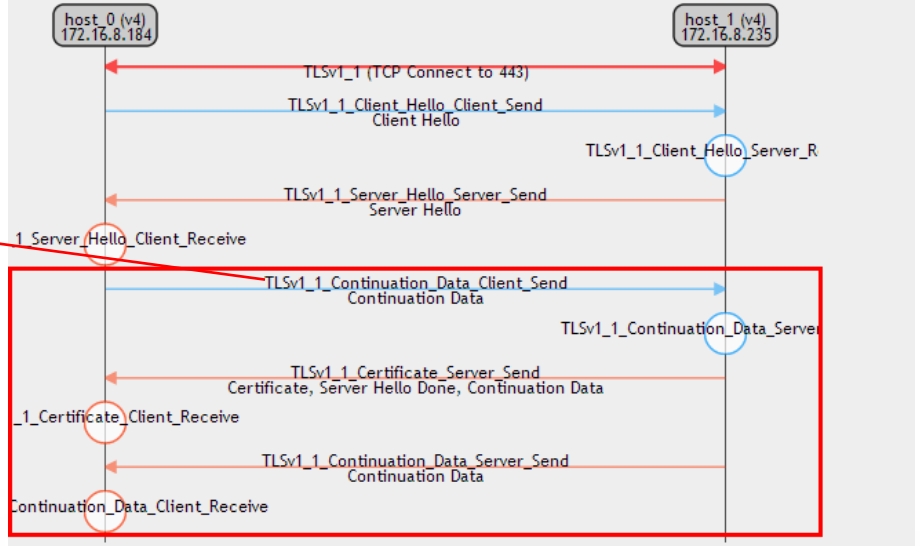
OpenSSL心脏滴血攻击流程展示

- 通过图形化交互流程形象的展示攻击流程
- 把攻击报文转换成开放的过程描述语言MSL

```
# Server Hello
TLSv1_1_Server_Hello_Client_Receive = TLSv1_1_Server_Hello_Server_Send.client_receive

# Continuation Data
TLSv1_1_Continuation_Data_Client_Send = TLSv1_1.client_send {
    0h180302000301ffff
}

# Continuation Data
TLSv1_1_Continuation_Data_Server_Receive = TLSv1_1_Continuation_Data_Client_Send.server_receive

# Certificate, Server Hello Done, Continuation Data
TLSv1_1_Certificate_Server_Send = TLSv1_1.server_send {
    # record|TLSv1.1 Record Layer: Handshake Protocol: Certificate
    struct [
        # record_content_type|Content Type: Handshake (22)
        22:8
        # record_version|Version: TLS 1.1 (0x0302)
        0x0302:16
        # record_length|Length: 614
        614:16
        # handshake|Handshake Protocol: Certificate
        struct [
            # handshake_type|Handshake Type: Certificate (11)
```

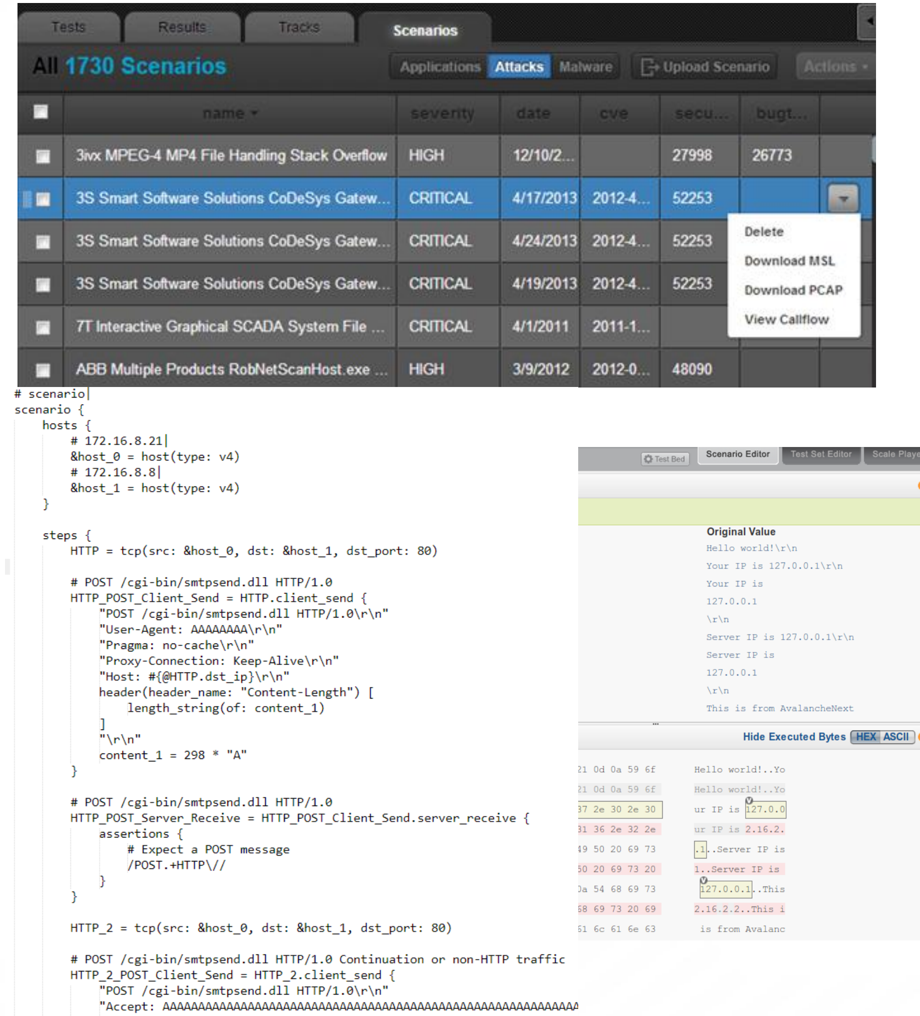
Callflow of [OpenSSL TLS DTLS Heartbeat Information Disclosure]

ID:	04.2014.04.20140408-01
Description:	An information disclosure vulnerability exists in OpenSSL. The vulnerability is due to an error when handling TLS/DTLS heartbeat packets. An attacker can leverage this vulnerability to disclose memory contents of a connected client or server.
Category:	Attacks
Hosts:	2
Steps:	11



用纯文本编写攻击和应用场景

- 提供描述两个主机之间多种协议交互的纯文本场景语言MSL
- 所有系统内置的攻击都可以导出MSL脚本
- 支持描述从2层到7层的简单和复杂场景
- KISS原则，用户只需描述关键部分
- 语言内置多达127种报文函数
- 用户可以根据现有攻击和漏洞编写新的攻击变种
- 编写私有0day漏洞，通过仪表检验网络靶场（Cyber Range）效果



恶意软件（Malware）测试

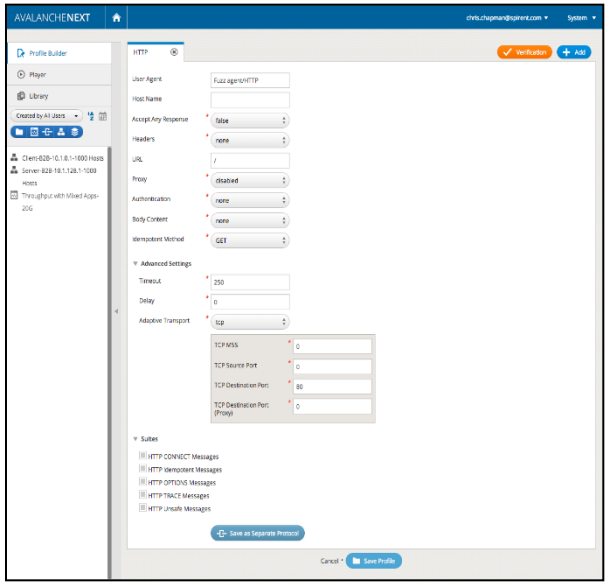
感染主机仿真	• 对于检测Malware的安全防范机制和策略进行测试
二进制代码传送仿真	• 测试恶意软件或者防病毒检测的有效性
在应用负载下的Malware测试	• 测试安全设备和策略在真实网络负载下的有效性和正确性

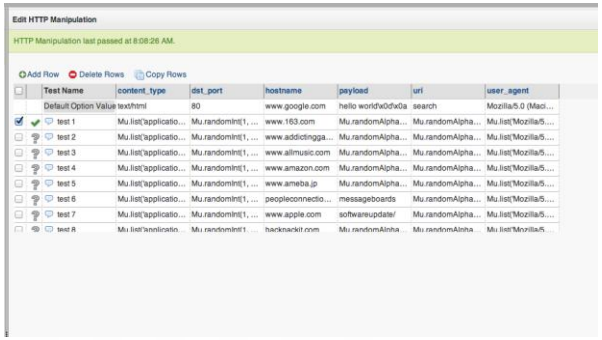
恶意软件测试

- Malware是不断发展的测试类型，建议每周进行新的Malware测试
- 通过Spirent TestCloud数据库，同步最新的Malware攻击手法
- 可以通过一个测试端口，同时进行Malware和正常应用流量混合模拟
  - 混合各种应用流量和Malware，并确保Malware被阻断
  - 通过同时模拟大量的应用特征状态机和Malware，测试真实世界场景
- 对于隔离测试，模拟受感染主机行为
  - 基于有状态的MuSL，Malware攻击不仅模拟核心攻击传送，而且可以模拟网络中受感染主机感染其它主机的行为
  - 当攻击开始被阻断时，则感染状态模拟也被阻止
- 高级根源分析
  - 分析系统显示未能被阻断的用户交互流程

协议模糊攻击 - Fuzzing

- 思博伦支持75种常见协议的Fuzzing测试，基于RFC协议标准，提供已经准备好的自动化协议测试机制。操作简单，不需要预备知识，只需要配置源和目标接口
- 主要协议举例
  - 二层协议 – ARP、IEEE 802.1Q/X、PPPoE
  - 三层协议 – IGMP、DHCPv4/6、IPv4/6、
  - 路由协议 – BGP、OSPFv2/3、IS-IS、RIPv1/2、MPLS、VPLS
  - VoIP 协议 – SIP、H.248、H.323
  - 加密协议 – SSH、SSL、TLSv1/1.2、ISKAMP、IKEv2
  - 工业控制协议 – IEC61850、MODBUS、DNP3，MMS
  - 应用层协议 – HTTP、SMTP、POP3、TELNET、LDAP
  - AAA – RADIUS、DIAMETER、TACACS+
  - 隧道协议 – VxLAN、GRE



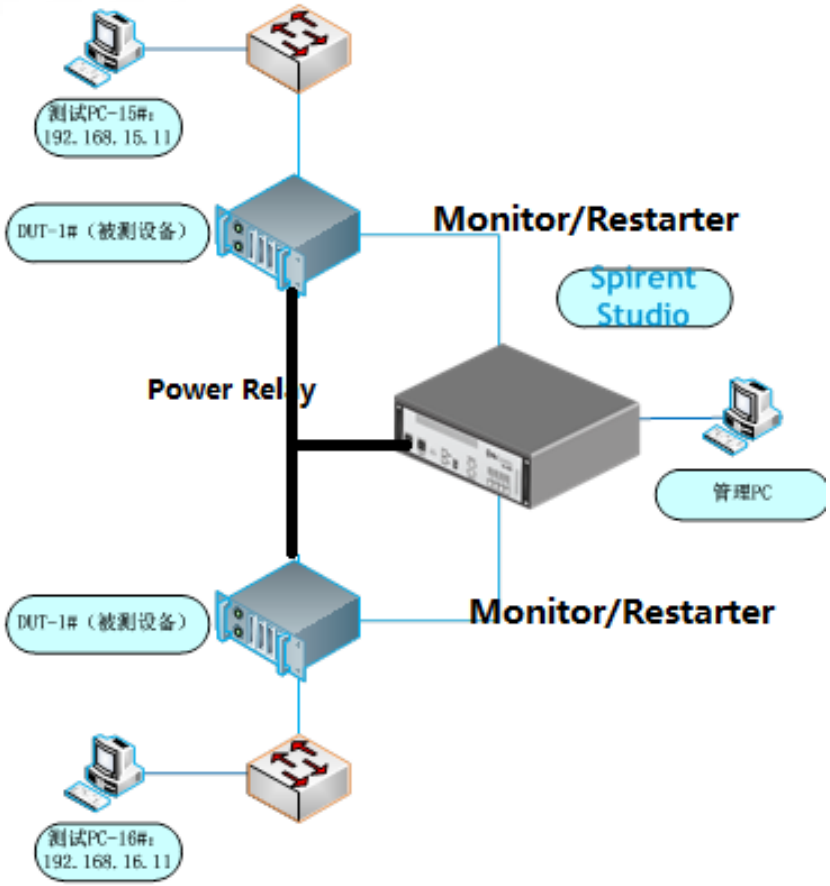


漏洞挖掘工具

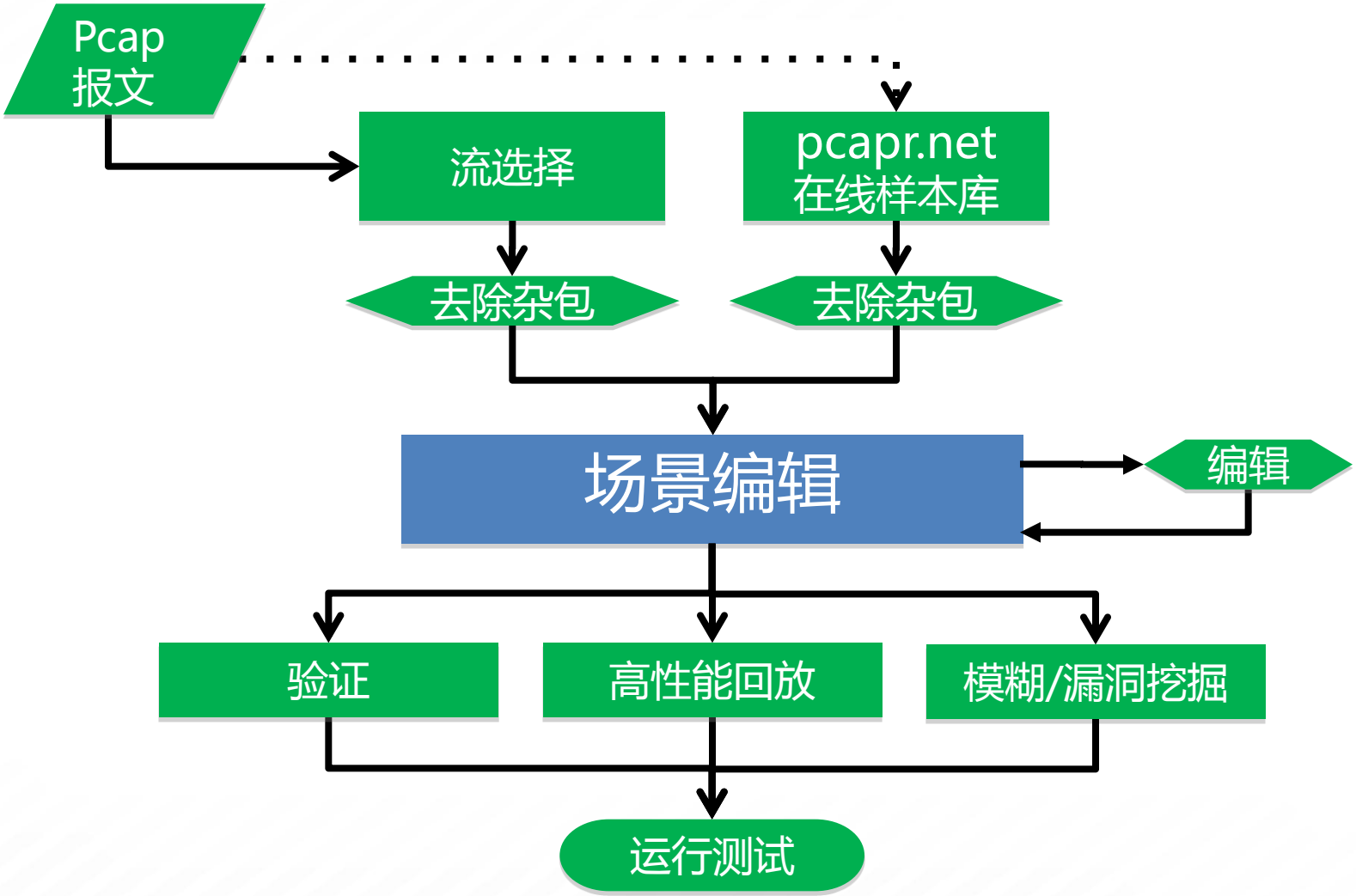
Fuzzing是进行未知漏洞挖掘/负面测试/健壮性测试的方法

在安全从业者保护用户的同时，黑客也在使用同样的方式寻找侵入的途径，这是一场无休止的竞赛，谁先取得先机，谁就占据了主动。

- **Protocol Mutation (Ground Up Protocols) (基于原生协议)**
- **Scenario Mutation (基于场景)**
- **调试及控制工具： Restarter, Monitor, EVT (重置器，监视器，故障可重现程序)**
- **支持测试自动化**

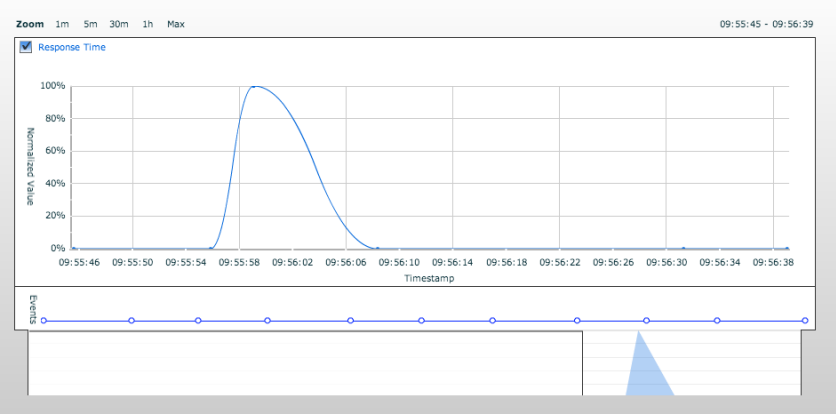


协议模糊测试工作流程


Pcap
报文
流选择
pcapr.net
在线样本库
去除杂包
去除杂包
场景编辑
编辑
验证
高性能回放
模糊/漏洞挖掘
运行测试

模糊测试结果分析报告

- 出了什么失败事件
- 哪里和什么时候出问题
- 失败事件相关的状态机
- 保存故障重现条件，可迅速重现故障



Executive Summary Report: ManfredP_dns_assertions.pcap

Mu System User	admin
Start Date/Time	7/2/12 4:46:35 AM
Duration	6 minutes 51 seconds 501 milliseconds

Product	Mu Test Suite (6.5.2.r48322)
Mu System IP	172.16.1.54
Mu System Serial #	0203-0711-0000-008E

Detection Effectiveness of Target

Detection Effectiveness Against Traffic Variations

Effectiveness F 6.534%

Test	Missed	Blocked	Effectiveness
ManfredP_dns_assertions.pcap	6,838	478	6.534%

Traffic Variation Results (Scenarios)

Grade A+ 100% > Five 9's

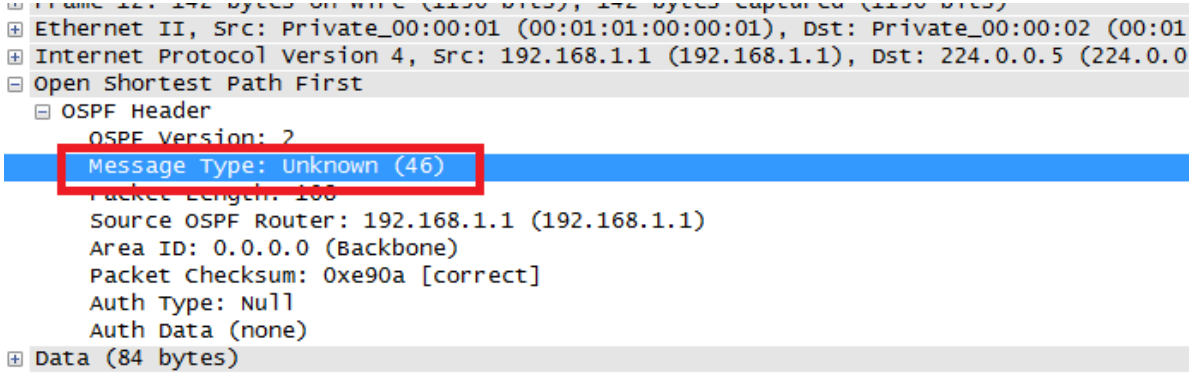
The target was analyzed using **7,317 variations** (generated from 174 test cases in 1 scenario). The target was **available for 6 minutes 48 seconds 704 milliseconds** during the attacks and was **unavailable for 0 milliseconds**.

Total Tests Run	**174** test cases were run
Passed	**174** test cases passed
Failed	**0** test cases failed

Test	Statistics	
ManfredP_dns_assertions.pcap	Protocol Scenario	ManfredP_dns_assertions.pcap
	Availability	100.000%
	Faults	No faults were found
	Variations	7317
	Coverage	

路由器Fuzzing测试举例

- 测试例及描述
  - OSPFv2 Messages-ospfv2.ls-update-mutated-1.header.type.**values**(16-23)
  - 该测试例主要是把OSPF Link State Update Messages 中的Message Type用其他异常值替换正确值4



- 现象：路由器不断重启
- 该类异常通过用异常取值替代正确取值，比如一个IPv4地址用多个换回地址代替，一个文本类型的参数用有符号整型值来代替等

仿真4000多种应用

Show Filters

Search Scenario

Business Systems 268	Communication 916	Games And Entertainment 161
Adobe, Sharepoint, MYSQL	Skype, IMAP , JAbber	Farmwille, Battlefield, Mafla Wars
Miscellaneous 478	**Network Protocols**	**P2P 853**
Fandango, eBay, Kayak		BitTorrent, Guntella, eDonkey
Productivity 242		**Streaming Media 793**
Box, Drupal, Google Finan		ix, Youtube, Pandora

应用流量仿真测试

- Native protocol，已经支持该应用的协议栈，直接使用
- 除了支持Native Protocol，SAPEE（可扩展的应用层回放仿真环境）支持各种P2P，Messenger以及私有协议测试
  - SAPEE提供多流多协议动态协议仿真，支持所有基于TCP/UDP的应用，基于SAPEE可以订制或者自定义任何可重用可编辑的应用协议库，SAPEE是应用生成工具。
  - SAPEE回放内容可以100%确保流程的准确性，通过SAPEE你也可以按照自己的要求对内容进行修改，也可以写你自己的私有协议。
- TestCloud/Store
  - TestCloud在线更新的4,000多种应用，包含国内常用的应用，会根据应用的版本进行周期性更新，按照需要进行在线更新。

攻击流量和正常流量混合测试

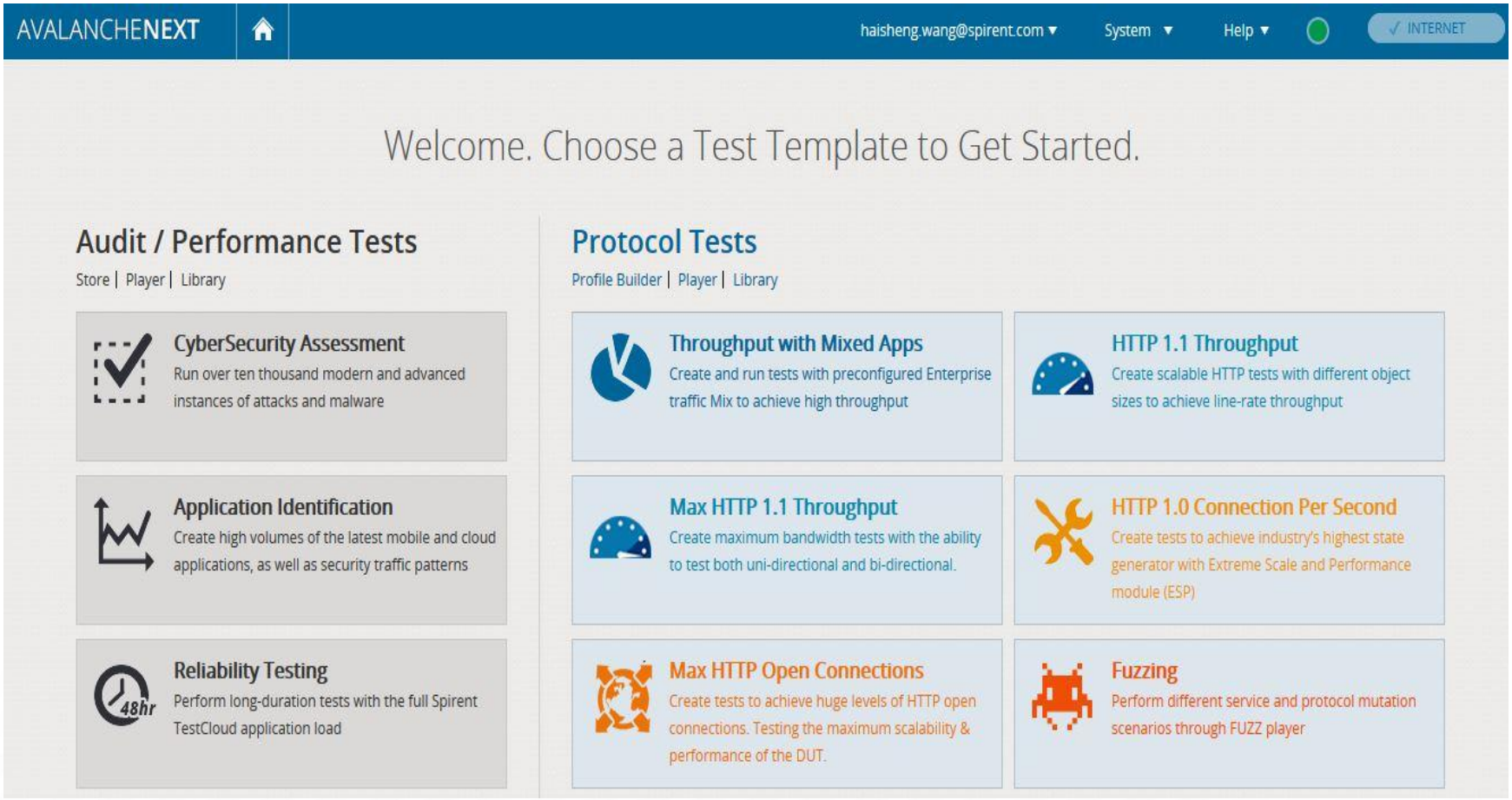
- 一些安全设备在单纯的攻击流量环境中，可以阻断所有攻击，但是当环境中同时混合了攻击流量和正常流量的时候，这些设备就会漏报一些攻击
- 在真实的网络中，没有单纯的攻击流量，所有的攻击都是和其它流量混合在一起的
- [RFC 3511] 5.5 Denial Of Service Handling – To determine the effect of a denial of service attack on a DUT/SUT TCP connection establishment and/or HTTP transfer rates.
- 网络安全设备测试的三个步骤：
  - 参考RFC 3511，测试安全设备的基准性能指标（并发TCP连接数、最大TCP连接建立速率，等）
  - 攻击流量性能测试
  - 攻击流量与正常流量混合 — 检查安全设备在检测和阻断攻击流量的同时，不影响其对正常流量的转发（无性能损耗）

思博伦下一代网络安全测试方案
Avalanche NEXT

- 基于Web浏览器的多用户界面
- 最新应用和攻击内容测试（Spirent TestCloud）
- 高性能：千万级并发连接数；百万级TCP连接建立速率（CPS）
- 攻击/已知漏洞测试
- 协议模糊攻击（Fuzzing）测试
- Malware仿真测试
- 测试方法学（RFC 3511）
  - HTTP CPS
  - HTTP 并发连接数
  - HTTP & E-Mix吞吐量测试

Avalanche NEXT

- 面向测试方法学的多用户界面



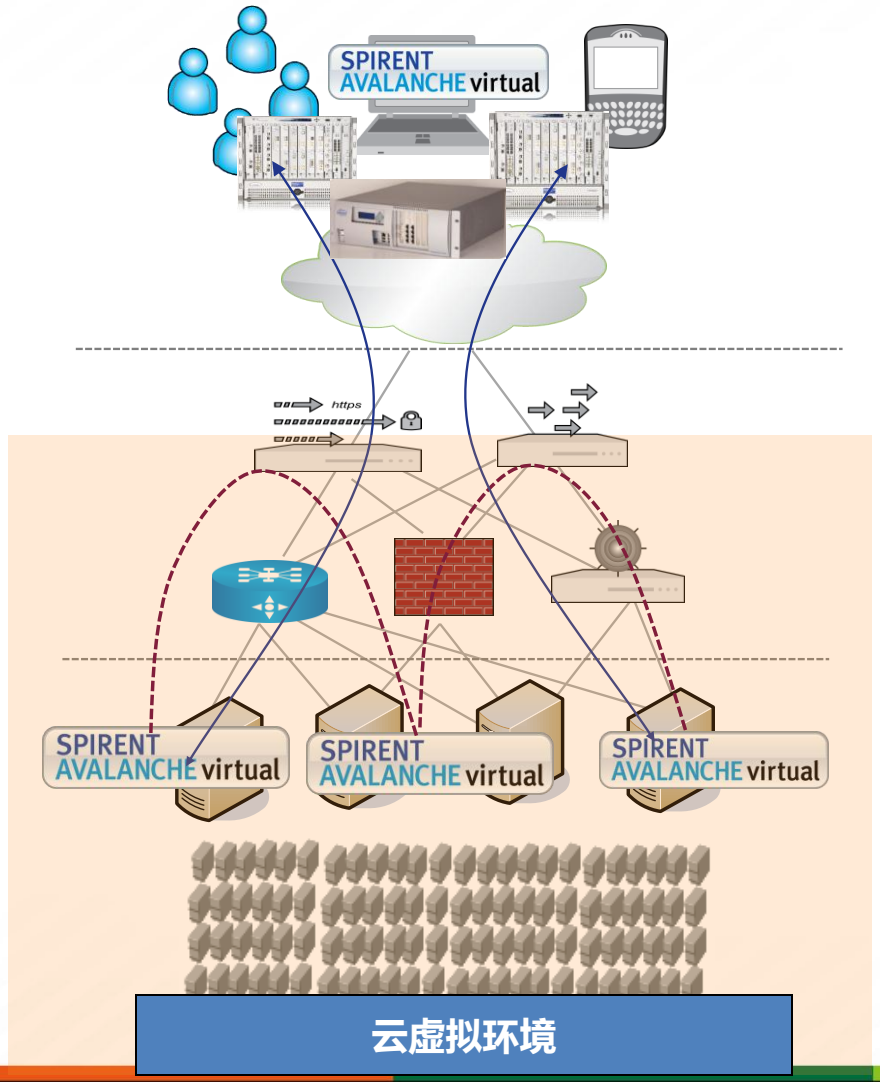
Avalanche NEXT测试对象

- 防火墙、应用防火墙、下一代防火墙
- 深度包检测设备（DPI）、同一威胁管理平台（UTM）
- 入侵检测系统/入侵防护系统（IDS/IPS）
- VPN网关（IPSec VPN、SSL VPN）
- 4-7层交换机、服务器负载均衡器（SLB）
- 网络缓存、代理缓存、Reverse-Proxy
- URL过滤设备、内容过滤器、SMTP中继
- 防病毒系统、反垃圾邮件系统、防间谍软件系统、防Malware系统
- SSL加速器、HTTP/HTTPS加速器
- 各种应用网关及IPv6支持
- 网络存储测试
- 虚拟交换机
- Openflow控制器和交换机

Avalanche NEXT测试对象

- 防火墙、应用防火墙、下一代防火墙
- 深度包检测设备（DPI）、同一威胁管理平台（UTM）
- 入侵检测系统/入侵防护系统（IDS/IPS）
- VPN网关（IPSec VPN、SSL VPN）
- 4-7层交换机、服务器负载均衡器（SLB）
- 网络缓存、代理缓存、Reverse-Proxy
- URL过滤设备、内容过滤器、SMTP中继
- 防病毒系统、反垃圾邮件系统、防间谍软件系统、防Malware系统
- SSL加速器、HTTP/HTTPS加速器
- 各种应用网关及IPv6支持
- 网络存储测试
- 虚拟交换机
- Openflow控制器和交换机

云基础架构测试



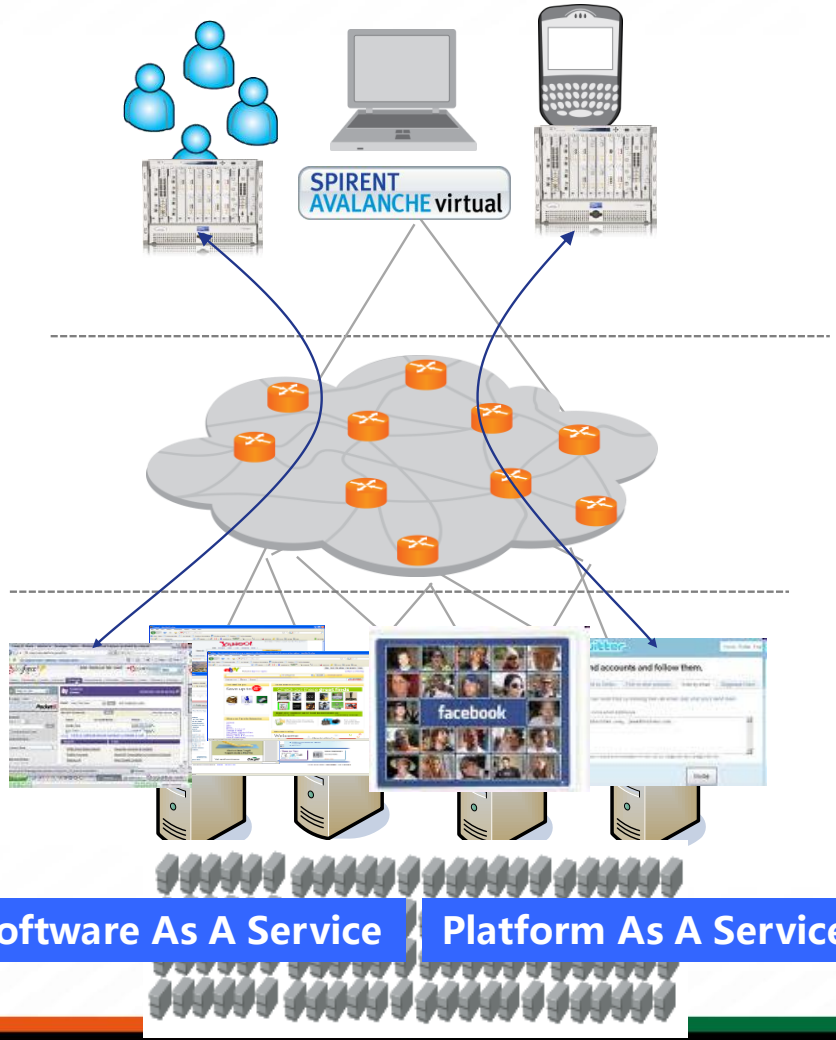
虚拟防火墙能够确保软件感染和恶意软件不会从一个虚拟机扩散到其它虚拟机吗？

虚拟负载均衡能够提供虚拟应用所需要的完全可用性和最大性能吗？

虚拟设备平台可以达到线速吗？

刀片服务器如何有效地支持多种应用？需要多少内存？

云应用与安全测试



如何将多个云服务平台合并？

云平台有效地维持线性扩展，并且承载基于需要的负载吗？

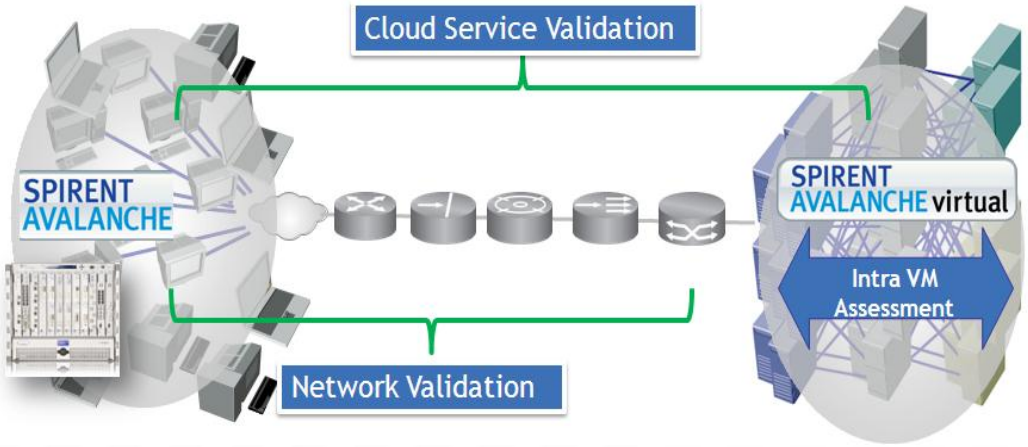
业务如何确保那些云网络中的可能的敏感信息是安全的？

现有应用在不做重新设计的前提下，可以被部署在云网络中吗？

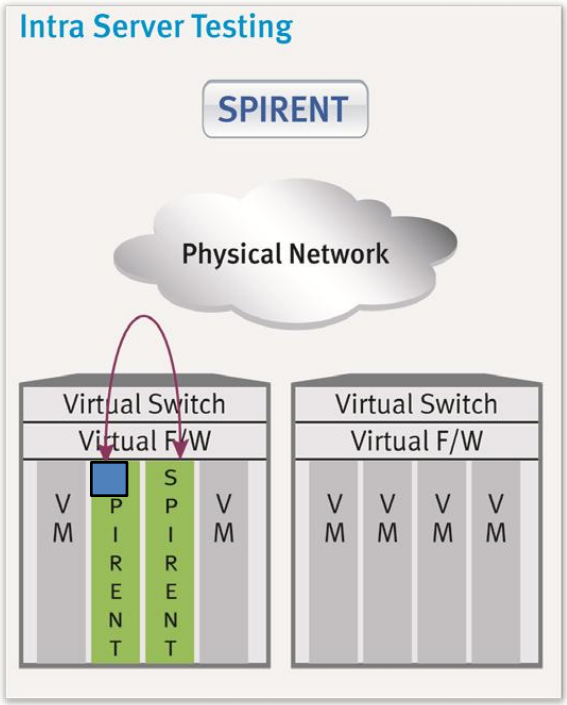
高可用性应用，如何保障持久性和容错性？

Avalanche Virtual

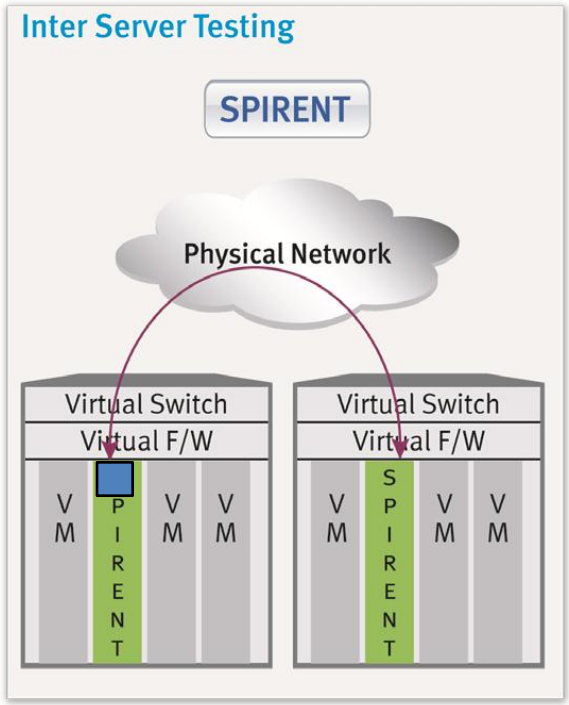
- 业内第一套云应用和安全测试解决方案
- 测试私有云、公有云、以及混合模式
- 具备思博伦应用与安全测试方案的所有功能，并且高性能
- 可以与Avalanche硬件进行协同使用
- 支持Avalanche Virtual Anywhere
  - VMWare
  - KVM
  - QEMU
  - Zen
  - Hyper V



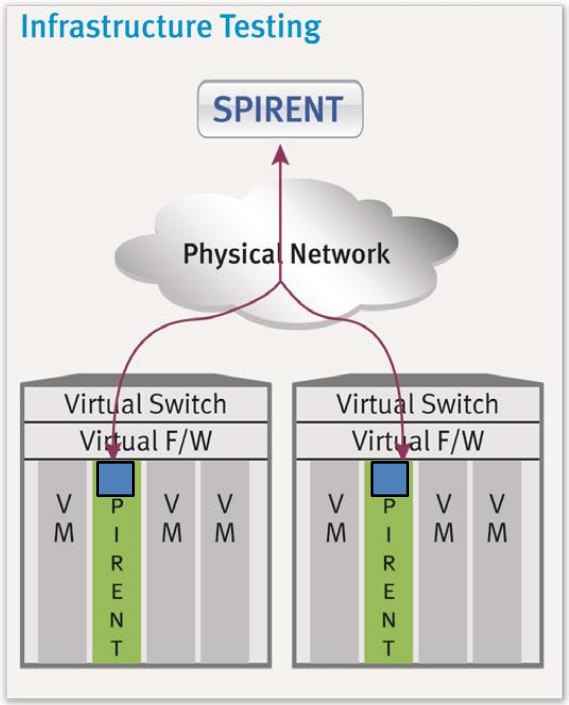
云安全测试拓扑



Virtual Port to Virtual Port



Virtual Port to Virtual Port
Across Virtual Switches



Virtual Port to any Physical Port

- 云应用和安全测试方案：Avalanche Virtual
- 三种测试模式：纯虚拟模式；纯物理模式；混合模式

思博伦网络安全测试总结

- 攻击仿真测试：已知攻击、未知攻击（Fuzzing）、恶意软件模拟
- 已知攻击测试手法更新：
  - Avalanche Attack Designer – 客户化定制攻击手法
  - TestCloud – 定期升级
- Fuzzing模糊攻击测试 – 未知攻击测试
  - Protocol Fuzzing – 已知协议Fuzzing测试
  - Scenario Mutation – 私有协议Fuzzing测试
- 海量应用仿真测试：SAPEE、TestCloud
- 高性能测试：千万级并发连接数、百万级TCP新建连接速率
- 线速应用流量仿真
- 安全协议（IPSec、SSL）性能测试、应用存储测试（CIFS、NFS）
- 云安全测试 – Virtual方案

Thanks!