第一届全国高校软件定义网络（SDN）应用创新开发大赛

决赛书面文档

华中科技大学联创团队代表队

指导老师
涂浩

参赛队员
陈康平
胡云锐
王兆麒
李英儒
白书来

2014 年 8 月　湖北　武汉

目录

1. 参赛情况

1.1. 参赛队伍信息表

队伍名称	联创团队		
领队姓名	周世伟	指导老师	涂浩
邮箱地址	shwzhou@hustunique.com		13164181545
所属学校（单位）	华中科技大学		
队员一	陈康平	队员二	白书来
队员三	胡云锐	队员四	李英儒
队员五	王兆麒	队员六	

1.2. 参赛队伍构成

1.2.1. 指导老师

涂浩

华中科技大学网络与计算中心讲师，工学博士。目前主要研究方向为下一代互联网、网络安全与大数据处理，作为技术负责人和骨干参与完成国家 863 计划、科技支撑计划、教育部、安全部、国家发改委 CNGI 及湖北省自然科学基金重点项目等多个项目，在相关国际会议和权威刊物上发表学术论文 10 余篇。

1.2.2. 联创团队

联创团队(Unique Studio)于 2000 年 6 月创建于华中科技大学，是以 Teamwork 和 Creation 为团队核心的学生团队。团队名称来源于"联众人之智"

必能"创辉煌之事"的信念。联创团队建立了一个自主的精英学生平台，在这个平台上学生自我管理，通过这个平台激发无限的潜力和创意。自成立到现在，联创团队已参加微软创新杯 11 次并 8 次进入全球总决赛拿下包括全球冠军等优秀成绩。除此之外，联创团队也多次参加各种大小型比赛并取得了骄人的成绩，并与微软、CSDN 等公司保持着非常好的合作关系，同时加入微软中国组织的创新联盟。联创团队多年的发展积累了独特的文化和运作机制，同时跟踪技术发展的最前沿，这使得联创团队在华科乃至全国高校中独树一帜。

1.2.3. 领队

周世伟

华中科技大学 2010 级本科生 ,现就读于光电与电子信息学院光电信息工程专业。

华中科技大学联创团队 IT 组&嵌入式组成员。曾 2 次获得国家奖学金。参与 Imagine Cup 微软创新杯 IT Challenge 比赛，并进入中国区总决赛。曾获得中国区第一届 RDMA 比赛一等奖。目前已获得华中科技大学保研资格。

个人博客：http://zhoushiwei1992.blog.163.com

1.2.4. 参赛队员

陈康平

华中科技大学 2012 级本科生，现就读于电子与通信工程专业。

华中科技大学联创团队队员。主要进行信号处理方面的研究。负责策略解释，将文本策略生成具体策略函数，以及单个动作函数 disconnect 的实现。

白书来

华中科技大学 2012 级本科生 ,现就读于计算机科学与技术学院信息安全专

业。

华中科技大学联创团队队员。主要进行网络安全方面的研究。负责 snort 日志分析（写入数据库）以及 snort 与 Pox 的通讯。

李英儒

华中科技大学 2013 级本科生 ,现就读于计算机科学与技术学院计算机科学与技术专业。

华中科技大学联创团队队员。主要进行服务器架构与分布式计算的研究。负责 AlertIn 事件处理函数的实现、按照策略层设计思路、动态生成的策略函数（解析事件参数、sql、时间戳）的调用实现、设计策略逻辑层及数据结构同时实现单个动作函数 reconnect、reset。

胡云锐

华中科技大学 2013 级本科生，现就读于计算机科学与技术专业。

华中科技大学联创团队 IT 组成员 ,主要进行网络通讯、大数据方面的研究。负责具体设计应用代码的架构、Pox 与 Snort 之间的通讯、AlertIn 事件的注册和各个模块之间的衔接、单个动作函数的 monitor、reset 以及 wait 函数的实现以及衔接之前 DNS app 的部分代码并调试应用部分代码。

王兆麒

华中科技大学 2013 级本科生，现就读于软件学院软件工程专业。

华中科技大学联创团队队员。主要进行 Android 端应用的开发。

2. 报告书

2.1. 应用简介和摘要

应用名称：自动化入侵防御系统（AIPS）

很多时候在企业网络安全，特别是服务器上数据库安全防范方面上需要特别注意，从而减少漏洞降低被入侵的风险。但是很多内网的防御都是外紧内松，一旦有一台主机被控制便会沦为跳板为后续入侵开辟连接通道，从而导致整个内网沦陷。

考虑到 OpenFlow 通过将网络设备控制与数据面分离开，从而可以对网络流量实现灵活的控制的特性以及 IDS 所具有的可以精确判断入侵事件并且可判断应用层入侵事件同时立即进行反应的特性，我们决定完成一个包含 snort 入侵检测系统的 SDN 内网，通过网关链接到 Internet，从而监测跟踪异常流量达到保护内部主机免受攻击或者处理已被攻击的 host 主机的目的。

2.2. 应用场景介绍

大型公司的内网为了防止被攻击，普遍会在入口处布置入侵检测系统以防止内网遭到攻击，但 IDS 并不是万能的，它存在以下几点权限：

- 深层攻击问题：虽然防火墙可以拦截低层攻击行为，但对应用层的深层攻击行为无能为力。

- 实时性低：IDS 可以及时的发现那些穿透防火墙的深层攻击行为，从而对防火墙进行补充。但 IDS 无法实时阻断的这一特点，导致大部分情况仍然需要维护人员人工检查系统。
- 协助不强 :防火墙技术和 IDS 没有一个统一的接口规范 ,不能够良好的协助。

而作为 IDS 的补充，IPS 的出现大大弥补了传统防火墙+IDS 模式的不足，IPS 与 IDS 的协作虽然解决了很多问题，但仍旧有以下不足：

- 横向流量：由于网络流量捕获受物理链路位置的限制，在无法大量部署的情况下，往往 IDS 及 IPS 只能部署在出口链路。这导致其只能捕获纵向流量，而不能捕获横行流量（即对内网的流量无从检测）。
- 成本问题：多链路部署 IPS 的行为会增加大量成本费用，并且防护 DDOS 类的流量攻击时需要消耗更多的资源和带宽，这严重的影响了网络效率。

传统网络的架构对入侵的检测依赖于对流浪数据包的分析，而且传统网络采用的是分布式的架构，将控制平面和转发屏幕耦合在一起，硬件则彼此分离。这样的设计导致想要实现网络拓扑内的流量监测相当困难。

因此我们引入 SDN 技术，通过 SDN 控制器的集中控制来实现流量的跟踪和策略化部署，并且整合安全工具真正实现自动化应对，这就是我们此次比赛的作品--AIPS（自动化入侵防御系统）。

系统结构示意图

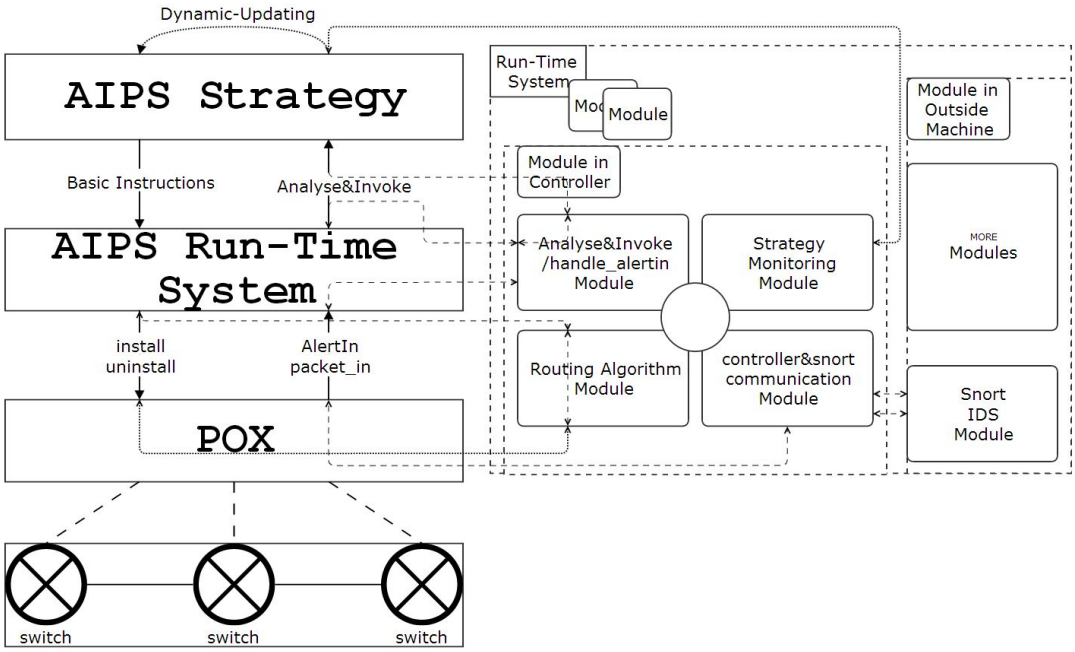
在我们的解决方案中，若检测到存在入侵流量之后，AIPS 会自动采取相对应的措施，让被攻击的主机所发出的流量重新经过入口供以 IDS 检测，并判断是否有异常流量，从而判断主机是否被入侵成功并保护其他主机不会遭到横向攻击。

2.3. 方案特色和创新

- 流量追踪：触发了警报的攻击流都会被镜像至 IDS 进行分析并对其进行重定向处理。
- 防御横向攻击：检测到存在入侵流量之后，AIPS 会自动采取相对应的措施，让被攻击的主机所发出的流量重新经过 IDS 进行检测，从而判断主机是否被入侵成功并保护其他主机不会遭到横向攻击。
- 正常服务不受影响：在防御措施运行的过程中，备用服务器将会启动并提供服务。
- 独创安全策略语言：利用一系列的基本动作实现更高级的安全控制和应对方案的语言，并且支持模糊匹配和动态更新。

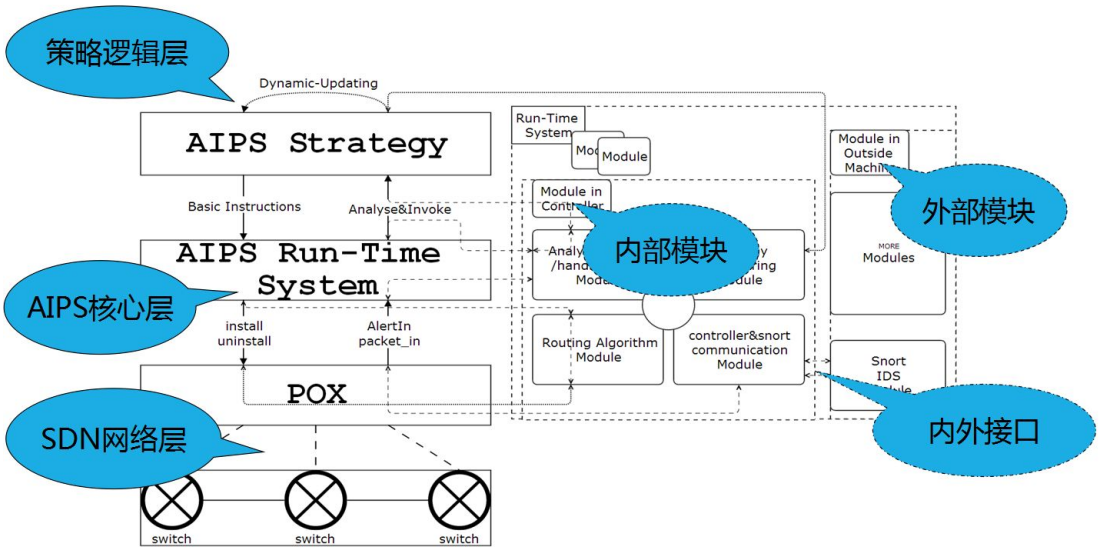
安全策略语言的基本动作

2.4. 应用具体设计论述



系统架构图

考虑到分层的设计可以降低层与层的依赖并且有利于各层逻辑的复用，我们采取了分层设计的思想，搭建出如图的系统架构。



AIPS 分层架构图

策略逻辑层（AIPS Strategy）：部署策略；通过与 IDS（snort）交互，编写安全策略；自动模糊匹配策略。

AIPS 核心层（Controller App）：与外部模块（IDS）通信；解释（向策略逻辑层提供接口）、执行（使用控制器的北向接口）策略；更改流表；路由算法；注册两个新的事件进入 POX 控制器内核，整合扩展其内核。

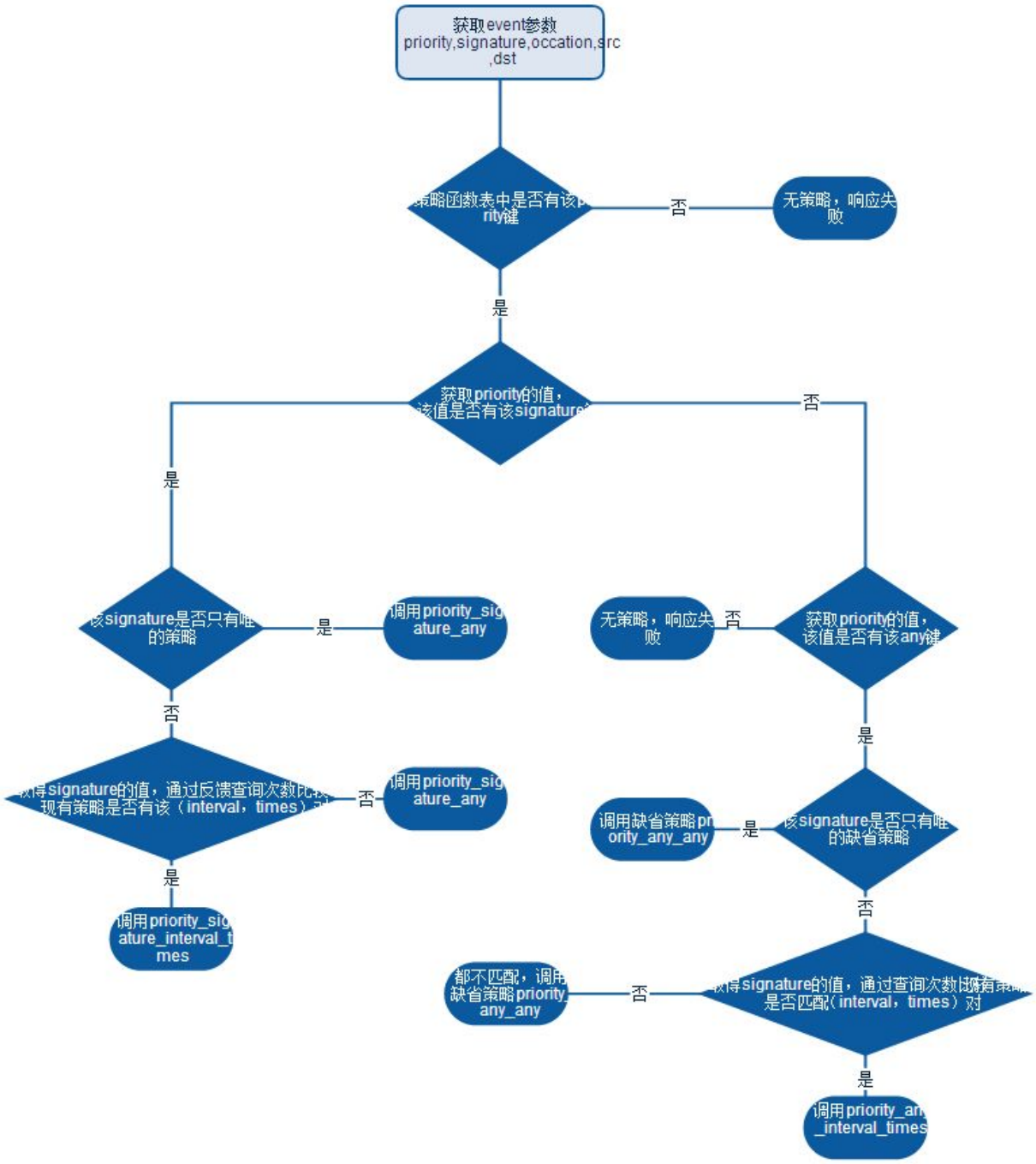
SDN Controller（网络层）：流表下发，与各 switch 交互。

内外部模块接口：运用自定义内外模块通信协议，核心层内部模块与外部模块 IDS 通讯；协助触发自定义 Alert_In 事件。

外部模块 :IDS 分析数据包 ,通过内外接口与核心层通信 ,间接触发 Alert_In 事件（安全工具等）。

各模块功能：

- 分析调用模块（handle_Alertin）：



（策略模糊匹配简化模型）

◆ 策略匹配与解释 :当捕捉到一个 AlertIn 事件时 ,将根据事件信息以及从 Snort 数据库查询到的结果 ,利用策略解释器进行解释 ,在 handlers 子类中查找最佳匹配的策略函数；若不匹配，执行多级缺省策略，达到警报模糊匹配策略的功能。（若为匹配到函数，会在 log 中出现 error：No Strategy for

$EventName）

- 策略执行与更新：根据解释结果，在一个新进程中将其调用，逐一执行策略函数中的基本动作；安全核心组件会根据事件信息的变化不断匹配新策略，在明确攻击类型的情况下，编写同族策略，攻击提供的警报可自动化皮这一同族策略，达到预期效果。

策略文件监视模块：

- 运用 inotify 监视策略文件夹，自定义监视事件处理器（FILE_Monitor_Event_Handler）,处理 Modified ,Moved_In ,Moved_Out，Delete 等事件，添加、更新、删除 handlers 子类中的同名策略函数，以达到即时动态更新策略的功能。

选路算法模块：

- 某些策略函数调用此模块，计算路径对相应交换机下发流表，以达到函数预期功能。

通讯模块：

- 监听 Snort 通讯：在初始化时打开一个端口供 Snort 远程连接，一旦 Snort 发来警报报文，将触发一个 AlertIn 事件同时传递其相关信息。
- 初始化部分：设置启动所必需的依赖，对各参数进行初始化同时注册并监听事件，启动安全核心组件，读取 rules 目录下已部署策略，再将每个策略解释成由 基本动作组成的函数并注册到 handlers 子类下的同名函数以供调

用。

基本目标：

- 可单点部署（POX 的 APP）。
- 可动态捕获/响应外部设备指定的网络流量。
- 可动态更新策略。

具体设计：

① 当外部流量通过网关进入内网并进入连有 Host 主机的子网络的时候，会经过 IDS 进行检测；

② 根据 IDS 的流量风险等级调用不同的策略进行处理，大致有如下几种情况：

a) 若 IDS 检测到危险流量，OF 控制器则会执行相应策略阻止攻击流进入，从而保护内网；

b) 若 IDS 检测到风险流量，OF 控制器会根据风险等级调用监视流量的去向、监视终端机的流量等策略，将终端机的流量重定向到 IDS 进行检测，并调用相应级别的策略进行处理。

c) 若 IDS 检测到正常流量，则让其正常通过。

2.5. 应用实现过程

程序流程：

- ✧ 启动所有虚拟机，并启动 Pox Controller（此时规则为空）。
- ✧ 在 Pox 上运行 AIPS。
- ✧ 若外网对 SDN 内服务器进行攻击，日志会记录此次攻击，并根据策略进行处理。
- ✧ 若内网主机对 SDN 内服务器进行攻击，日志会记录此次攻击，并更具策略进行处理。
- ✧ 若需要更新策略，只需要将策略文件移动到对应位置，无须重启，即时更新系统。

实验设计：

演示系统的通讯机制、处理机制、配置文件的内容、匹配方式和动态更新功能。实验拓扑为 controller+ovs+gateway+lds+httpserver+backhttpserver+外网恶意机器。

演示步骤：

- ✧ 启动所有虚拟机，并启动 Pox Controller（此时规则为空）。
- ✧ 使用 ping，确认网络正常。
- ✧ 在 pox 目录下新建文件，内容为

  monitor,dst

  redirect,src

（文件名为 3_Not Suspicious Traffic_any）

此处演示 monitor、redirect 动作。

- ✧ 外网访问一号服务器，网页显示为一号。
- ✧ 在没有策略与之匹配的情况下显示"No Strategy for 03"。
- ✧ 此时将 pox 目录下的 3_Not Suspicious Traffic_any 移动到 pox/rules 目录下，可以发现日志显示规则被更新了，这说明我们的 AIPS 是即时动态策略更新的，此功能可以在不重新启动系统的情况下即时应对出现的新问题，并为将来的智能安全分析策略生成提供基础。
- ✧ 用外网虚拟机 telnet 远程登陆 httpserver，可以发现日志显示 Alart_in，并使 httpserver 的流量经过网关以供 IDS 检查
- ✧ 由于流量没有被阻断，外网恶意机器成功登陆到了 httpserver 上，恶意机器以 httpserver 为远程跳板试图登陆上 backhttpserver 上。
- ✧ 可以发现日志记录了这次攻击，httpserver 被断开，去向 httpserver 的流量被重定向到了 backhttpserver 上。
- ✧ 并且在此过程中启动了备用服务器提供服务，这体现了本系统安全功能并不会影响正常的服务。

此处演示规则匹配方式

- ✧ 在 pox/rules 文件夹下创建 03_ICMP Echo Reply_2,内容为：

  Disconnect，dst

  Wait，30

  Reconnect，dst

可以发现日志显示规则被更新了

- ✧ 使用外网主机 ping SDN 内任一主机一次后立即停止，发现网络内没有任何变化。
- ✧ 使用外网主机再次 ping SDN 内同一主机，发现 SDN 内主机被断开。
- ✧ 更改文件名为 03_any_2 重复以上实验，发现结果不变。

2.6. 强大的可扩展性

- ■ 策略更新机制：由于策略可以随时更新，我们只需通过导入新的策略而不必更改系统其他配置，保证了系统稳定而不影响正常服务；
- ■ 外部模块替换：snort 在我们的抽象中作为 AIPS 的安全模块，因此可以替换为符合 AIPS 的外部接口协议的一个或多个安全工具以适应不同需求，也可以利用安全策略语言的优势引入其他模块；

3. 附录

演示性材料：AIPS 演示.pptx

源代码：代码.zip

相关数据及图表：document.doc

文档：SDN-联创团队.pdf