An SDN-Supported Collaborative Approach for DDoS Flooding Detection and Containment

Milcom 2015 Track 3 - Cyber Security and Trusted Computing

监视器→相关器→控制器

（1）当发生攻击时，监视器发出警报；分布在计算机网络上的监视器不断地观察网络流量是否有任何异常。

（2）通过警报通知，网络攻击相关器进一步评估情况，如果需要，识别攻击者的位置和攻击路径；位于OVS的相关器根据需要响应来自监视器的警报。

（3）如果适用，OVS控制器采取缓解措施阻止攻击流量或重新路由攻击包。SDN控制器本身采取措施修改网络流量以缓解攻击。

观察SYN请求：

一种模式是SYN请求激增，因为此攻击试图耗尽受害者计算机上连接缓冲区中的网络资源。我们可以根据统计流量基线为监控器设置控制阈值，以便在出现此类增长时快速发出警报。

不幸的是，正常的网络流量转移也会增加SYN请求。因此，仅此模式并不是SYN洪水攻击的唯一模式。仅依赖此症状可能会产生错误警报。

监控功能（监视器）：

异常检测引擎有两个重要的优点。

首先，它基于一个正常的行为模式，即一个可以作为正常流量统计抽象的预期基线。因此，监视器不需要处理单个网络包。这有助于降低计算成本。

其次，该检测方法是稳健的，因为它是基于识别与既定基线的偏差，例如，超过控制阈值的TCP SYN包的激增。因此，它可以快速标记网络流量中的任何异常情况，甚至新类型的攻击，代价是生成错误警报。

相关器：

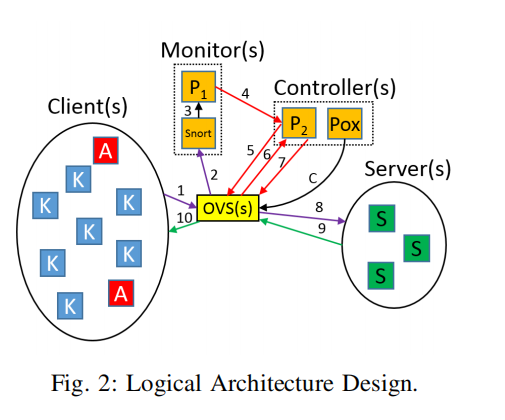
一旦收到警报，相关器就会根据警报类型立即采取行动。通常，相关器需要首先收集额外的数据包和数据以获取相关信息。仔细检查证据后，如果相关器不能识别攻击者，这可能仅仅表明正常流量的增加。然后向报告监视器发出重置命令。根据需要更新正常流量状况，以建立新的基线。

控制器：

最后，对攻击存在的确认又会按计划触发攻击遏制行动。这些操作可以由SDN控制器执行，范围从丢弃攻击数据包，到部署蜜罐以欺骗攻击以获取更多证据，到动态重新配置网络和重塑流量。

监视器监视所有进入网络的流量

系统架构



在图2中，节点A被定义为攻击者，K是合法用户，S是客户机-服务器模型的服务器，其中A和K是客户机。网络链路（2）配置为镜像端口，通过该端口，通信将单向从OVS传输到监视器。因此，监视器监视所有进入网络的流量。（2）的配置被设置为单向，以防止基于TCP通信的循环机制。

当A和K与网络（1）通信时，信息被转发到监视器（2）和服务器（8）。监视器接收到流量（2）后，使用入侵检测系统（IDS）snort处理信息。如果snort发出警报，则将信息（3）传输到p1以通知（4）控制器。在监视器上运行的通信器算法p1正在不断地实时监听警报。它是轻量级的，可以管理警报和其他相关信息。一旦IDS发出警报，P1就会使用针对特定类型攻击的简单攻击标志通知相关关联器。然后监视器收集与攻击相关的最少数量的信息，并将其发送到相关器。

通过检查源自发送OVS端口的IP地址的数量来进行关联。我们假设在一个DDOS攻击模型下，源IP地址将随机分配给发送的每个数据包，相关器不会受到影响。在p2中，决策树用于从上（1）丢弃任何未来的流量。然后将决定（7）传输到OVS。如果确定（1）发送的流量被认为是恶意的，则通过（7）上的操作进行预防，并且流量将永远不会到达（8）上的S。如果流量被认为是出于良好的目的，信息将被传送回客户（9，10）。当（9）发生时，根据镜像端口的设计，在（2）和（10）上传输流量。

如果p2未检测到欺骗的IP地址，则监视器的警报为假警报。这可能是由于ID的敏感性和/或正常流量的增加造成的。可以采取纠正措施来更改ID的警报阈值。