EPON 安全问题探悉*

赵 丹[1], 朱 娜[1], 赵 红[2]
(1. 江苏大学 计算机科学与通信工程学院, 江苏 镇江 212013; 2. 浙江工业大学 信息工程学院, 杭州 310014)

摘 要: 以太无源光网络(EPON)的点到多点(P2M)结构使其存在严重的安全隐患。结合具体的 EPON 结构和原理,全面详细分析了 EPON 系统中各种安全攻击(从简单的被动监测到拒绝服务(DoS)、再到伪装和窃取服务(ToS))实施的原理、过程及其危害性,并提出了相应的对策,包括鉴定、安全封装、加密、入侵检测、利用到期活动等。

关键词: 以太无源光网络; 安全; 窃听; 拒绝服务; 伪装; 窃取服务; 加密
中图分类号: TN929.18 **文献标志码**: A **文章编号**: 1001-3695(2009)02-0719-04

Analysis and research on security of EPON

ZHAO Dan[1], ZHU Na[1], ZHAO Hong[2]
(1. *School of Computer Science & Telecommunications Engineering, University of Jiangsu, Zhenjiang Jiangsu* 212013, *China*; 2. *School of Information Engineering, Zhejiang University of Technology, Hangzhou* 310014, *China*)

Abstract: Ethernet PON (EPON) system has serious security issues for its particular P2M(point to multi-point) architecture. This article analyzed the implementing theory, process and harm of all major security attacks, including simple passive monitoring, denial of service (DoS), masquerading and theft of service (ToS) inherently presented in EPON systems in detail. And presented corresponding countermeasures, such as authentication, so-called secure packaging, encryption, intrusion detection and utilization of time-out events etc.

Key words: EPON; security; eavesdropping; DoS; masquerading; ToS; encryption

近年来,随着 Internet 的普及和宽带应用型业务的大量涌现,用户的带宽需求日益增大。而核心网络和用户驻地网的速度都达到吉比特级别,接入网部分又沦为整个网络的瓶颈。FTTH(光纤到户)作为接入网的最终理想,已经被人们重视并开始大量应用。以太无源光网络(Ethernet passive optical networks, EPON)是 FTTH 各种传输方案中性价比最高的一种,用来给大量个人或商业用户提供传输安全敏感型数据的服务。由于其特有的 P2M(点到多点)结构及传输媒介的广播特性,使得其具有特殊的安全需求。下行广播通道能被任何想窃听的组织秘密访问,只要去掉光网络单元(ONU)的逻辑链路标志(LLID)过滤规则,使其工作在所谓的混杂模式下,即可访问所有的下行数据流。从 EPON 的具体结构出发,从研究 MPCP(多点控制协议)及其对系统安全的影响入手来全面分析安全问题。

1 MPCP(多点控制)协议

由 IEEE 802.3ah 任务组开发的多点控制协议(MPCP),是用来解决与在 EPON 系统 P2M 环境上进行 P2P 以太网操作相关的问题。EPON 系统中使用所谓的仲裁机制来动态分配到各 ONU 传输介质(光纤通道)的访问权,从而给各个活动附属设备动态分配上行传输时隙。如果能保持网络的固定运行环境,使链接的 RTT(round-trip time,往返时间)稳定,那么所分配的时隙总是会不重叠的,即它们到达 OLT 收发模块时,数据帧可以被正确接收、成功描述和解码,这样就在用户和 EPON 连接的高层网络(MAN/WAN)之间提供了数据传输通道。MPCP 提供了完整的信号设备(所谓的控制板),协调从多个活动 ONU 到 OLT 接收器之间的数据传输(这样上行方向是 P2M 操作模式)。

MPCP 机制的运行原理可以描述如下:采用 TDM(时分复用)技术,将整个可用上行信道带宽分为各个传输单位(通常称为时隙),用 OLT 中心的包调度器的运行机制下的 DBA(动态带宽分配)机制分配给各个活动 ONU(更具体地说是各个 LLID)。包调度器为各 LLID 分配上行传输时隙,它依赖于给定实体(如使用 REPORT MPCP DU)的当前带宽需求、可用带宽、其他 LLID 的带宽需求、LLID 数、采用的服务策略等;然后用相应的 GATE MPCP DU 通知 ONU 传输时隙的大小和开始时间。

MPCP 传输机制基于两个信息帧,即上述的 REPORT 和 GATE MPCP DU。REPORT MPCP DU 由 ONU 发出,用来向 OLT 描述当前带宽需求。带宽需求一般基于当前拥有的队列(一个 ONU 可以有多个存储以太帧的包队列,与多个可用 LLID 实体对应[1])。由于 MPCP DU 预先定义了有限大小,一个 REPORT MPCP DU 可拥有的报告队列的最大值为 13。IEEE 802.3ah 标准允许存在所谓的队列阈值(queue thresholds),使 ONU 能够表示每个队列的描述界限,通过在每个具体队列的内部结构提供额外信息,提高 OLT 端的调度效率。这

收稿日期: 2008-04-17; 修回日期: 2008-07-12 基金项目: 国家自然科学基金资助项目(60702056); 镇江市科技计划资助项目(SH2007070)

作者简介:赵丹(1982-),女,浙江台州人,硕士研究生,主要研究方向为光接入网技术(zhao2dan@sina.com);朱娜(1957-),女,江苏镇江人,教授,硕导,主要研究方向为光通信技术;赵红(1982-),女,浙江台州人,硕士研究生,主要研究方向为移动 IP.

种机制在前述标准中从未被详细阐述过,其实施是对系统开发商公开的。

一旦 OLT 端接收到 REPORT MPCP DU,就对它进行解析后传给 DBA 模块,DBA 再负责安排上行传输时隙的大小和开始时间,要使得来自多个 ONU 的传输在 OLT 接收端不会重叠。每个分配的时隙的大小取决于实际带宽需求、选择的服务策略(用的是静态还是动态带宽分配)、活动 LLID 数、可用带宽数、使用的轮流检测协议等。该 MPCP 被设计成能运行任意的 DBA 机制,从而为开发各种复杂的新带宽分配协议提供一个共同的控制板。一旦 DBA 模块完成时隙的大小和时间估计过程,一个 GATE MPCP DU 就构造好了。其中装有各自的 DBA 评估信息,并在第一个可能的时间在下行传输(以太网帧不能被割裂,因此所有 MPCP DU 以最高优先级传输,虽然可能在传送时排在一个长帧后面)。按照 IEEE 802.3ah 标准,一个 GATE MPCP DU 使得中央的 OLT 控制器一次最多调度四个传输时隙(即所谓的 scheduling into the future),其尺寸为 2^{16} - 1 TQ(对于 1 Gbps 有效数据速率,1 TQ = 2 B = 16 ns),从而一个单个传输时隙限于约 128 KB。收到这种 MPCP DU 后,ONU 使用信息帧中的时间戳更新它的本地时钟索引,从而有效地维护与 OLT 时钟的全局同步,而无须一个单独的时钟信号。调度信息被相应地解析和加工,由此造成传输事件产生,一旦本地时钟值达到时隙开始值,如前面处理过的 GATE MPCP DU,就会开始传输。在传输时隙,当前 ONU 利用其本地的内部 ONU 调度器传输存储的以太帧,在分配时隙内尽可能多地填满。由于以太网帧不能割裂,且划定范围通常在 REPORT MPCP DU 传送及接收各个 GATE MPCP DU 之间变化,就产生未使用的时隙残余,从而造成上行信道传输某种程度的低效[2]。不符合当前分配时隙大小的其余的帧将被推迟到下次 OLT 调度器授权的传输机会。

除了传输调度,MPCP 也有许多其他功能,对正确操作 EPON 系统很重要,即自动发现、注册和为新连入的 ONU 测距(RTT 计算),这些组成了所谓的发现过程。在发现过程中,新连入的 ONU 允许注册到网络中,OLT 能获得关于它们距离和容量(可以排队的授权数、物理传输参数等)的信息。发现过程本身是很复杂的,特征是被称为发现窗口的一段时间。在发现窗口内,所有的标准数据传输均停止,只允许异步传输来自新连入 ONU 的 REGISTER_REQ MPCP DU。其中该 ONU 至少有一个未注册的 LLID 实体。这个过程是由特定的 OLT 实体驱动,它定期使得发现窗口可用,广播那些 discovery flag(发现标志)为可用的 GATE MPCP DU,包括发现窗口的开始时间和长度。发现窗口是几个 ONU 可以以异步的方式同步访问上行信道的惟一的一段时间,因此原始传输可以重叠,导致包冲突,需要在下次发现窗口重新注册。为了减少传输重叠,所有的 ONU 均用一个竞争的算法——随机延迟机制(random delay mechanism)来解决,即在分配的发现窗口内等待一个随机数的时间单元再传输 REGISTER_REQ MPCP DU,这样可以减少包冲突的概率。因此在一个发现窗口内,OLT 可以收到一个以上的有效注册请求。

一个有效的 REGISTER_REQ MPCP DU 包含 ONU 的 MAC 地址和最大可授权数。当收到一个有效的 REGISTER_REQ 帧时,OLT 注册 ONU,分配并指派新的端口标志(LLID),并将相应的 MAC 地址与 LLID 绑定:之后,需要通知 ONU 成功接收注册请求,这是通过使用包含新近指派 LLID 号的 REGISTER MPCP DU 和 OLT 必须的同步时间(物理层参数)来完成。此外,OLT 回应有待解决的最大授权数,这预示着该信息被正确接收,并即将开始调度过程。其次,为新注册 LLID 预定一个 GATE MPCP DU,允许特定 ONU 在上行传输 REGISTER_ACK MPCP DU,完成注册过程。注册阶段的具体过程和 RTT 测距可参见文献[1,3]。

2 EPON 中的窃听

EPON 中,只要将其中一个注册过的 ONU 的工作方式设置成混杂模式,就可以在下行方向进行窃听了。因为网络中的每个 ONU 均接收 OLT 发送的(更确切地说,应该是 OLT 广播的,因为下行通道是 P2M 的)下行方向的数据包的一个拷贝,而 ONU 硬件无须进行扩展修改就可设置成混杂模式。攻击者所要做的仅仅是使 LLID 过滤规则失效,就可以自由地访问下行通道传输的所有信息了。更糟的是,所用的窃听方法完全是被动的,OLT 无法检测到,且在网络结构或性能上不会触发任何可察觉的负面影响;更为严重的是,它可以每天 24 小时、一周 7 天不间断而不被发现。这无疑违背了数据保密和隐私原则。

在上行通道,网络特有的硬件结构能阻止用户窃听来自其他位置的数据,因此用户数据较安全;同样地,就被动检测而言,上行通道被认为是安全的。只有 OLT 能接收和检测到各个 ONU 的活跃期。文献[4]中提出,目前传输路径上的被动分配器能够引入足够的信号反射(经放大)来重建从其他 ONU 开始的上行传输。但直到现在,这种机制也才被实践证明是可行的,现有信号反射强度能在噪声等级之上抽取有用信号。

这种机制能否被应用到实际中还未确定,需要进一步研究(包括信号强度的测量)。另外,这种反射型上行传输的波长不同于下行,虽然 ONU 不需要完全调谐的接收器,但恶意用户却可以通过操作两个带精确调谐接收器的 ONU 来绕过这种限制。

此外,由于 PSC(passive splitter combiner,无源光分路器)单元被制造成一个完全交互的设备,它本身就构成了一个极为严重的安全威胁。因而,即使只有设备的一个端口与主通道连接,更多没被连接的端口也可以被访问。用户定制设计的设备可以连接到 PSC 的没被使用的这种端口,提供权限访问用户和系统敏感数据,将光信号传输给流量分析器。随着 PSC 封装工艺的提高,可以使用一种安全封装法(即只有一个主端口和预先设置数量的端口可以使用,而其他端口隐藏在密封盒里)来阻止目前的这种窃听。这样,就不能访问其他端口,如果试图未经授权就访问上行通道的信号,将会毁坏设备而需要打开盒子。图 1 是目前的一种安全封装型 PSC 模块的内部结构,包括一个输入和几个预先设置数量的输出端口。

窃听是一种典型的网络初始阶段攻击方法,它以整个 EPON 网络结构为目标,获取访问传输媒介的权限。通常被认为是一种准备阶段,使用简单而完全透明的数据挖掘技术,攻击者就可以获得各种类型的敏感信息:从用户数据(隐私)、用户活动周期(在随后的 DoS 或 ToS 攻击中使用)、系统敏感数据(如 LLID 和系统中各个 ONU 的 MAC 地址)到轮流检测协议设置(可以从 GATE MPCP DU 及其内容中估计得到)。获取上述各种类型的系统和用户敏感数据后,攻击者可以进行更可见的、更有破坏性的安全攻击(即伪装、DoS、ToS 等),接下来将进行详细描述。

3　EPON 中的拒绝服务

3.1　EPON 下行传输

在下行方向, OLT 广播的以太包经 1 ×*N* 的 PSC 或 PSC 级联到达各 ONU, 每个 ONU 收到每个下行数据包的拷贝。接入的 ONU 的数目因可用预计光强度的不同为 4 ~64。其中 16 是 IEEE 标准规定的一般值(实际使用通常包括 32) 。PON 系统的下行通道的属性使得网络成为共享介质网络: OLT 广播的包到达各 ONU 后, ONU 根据 MAC 和 LLID 地址进行选择过滤。下行通道的工作过程如图 2 所示, 各种广播数据流中的包经 ONU 过滤后最终被送往不同的终端用户。

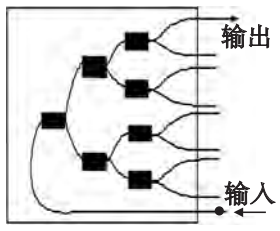

图1 安全封装型PSC 模块的内部结构

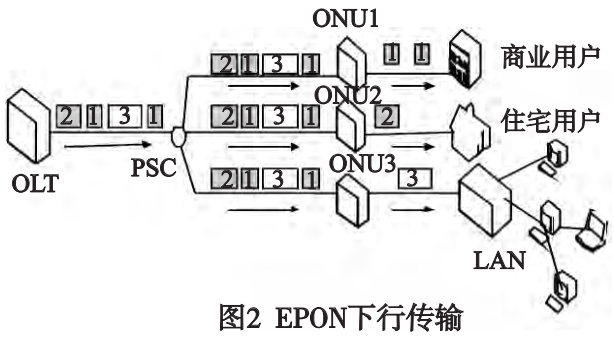

图2 EPON下行传输

3.2　EPON 上行传输

上行方向(图 3) , 从 ONU 到 OLT, EPON 的工作模式是 M2P, 即多个 ONU 将数据包传给一个 OLT 中的接收器模块。此外, 由于各 ONU 不能知道其他 ONU 的传输(PSC 是单向设备, ONU 看不到其他 ONU 在上行传输的信号) , 其连接性与 P2P 结构相似, 集中管理上行通道的访问, 在一个时间段内只允许一个 ONU 发送数据包。然而, 由于所有 ONU 均属于一个冲突域, 需要集中管理机制(一般通过一个 DBA 算法) , 默认状态的 ONU 不允许传输任何数据, 除非由 OLT 授权。这样, 在任意时刻中心的 OLT 控制器可以发现各个 ONU 的预订传输, 数据冲突就可以避免了。这种集中管理的上行访问策略的惟一特例是发现过程, 它允许新接入未初始化的 ONU 注册。

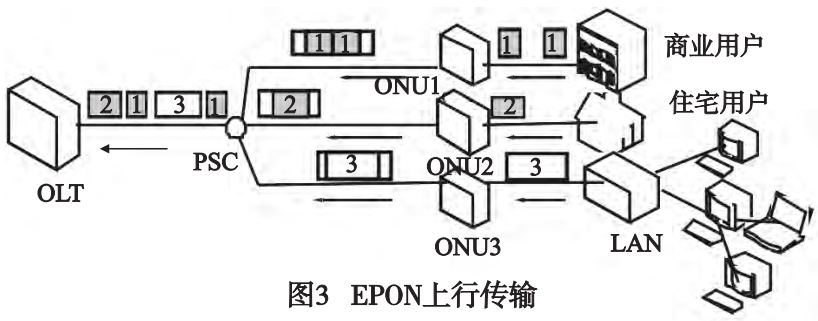

图3　EPON上行传输

EPON 是 M2P 网络, 每个 ONU 直接与 OLT 交互, 因此在上行方向需要多路存取访问协议, 基于竞争的媒介访问机制(与 CSMA/CD 相似) 很难实施[1,5] 。在一般的网络调度中, ONU 无法检测到 OLT 端的冲突, 在 OLT 与每个 ONU 间采用反馈回路在经济上是不可行的。基于竞争的机制在提供非确定业务方面有着明显的缺点, 如节点吞吐量和通道利用率可能被描述成静态的平均值, 那么在一个很小的时间间隔内, 不能保证 ONU 访问媒介, 即表示这种访问协议不适合延迟敏感的传输, 如视频会议和 VoIP。为了引进帧传递中的决定性, 文献[6 ~9] 中提出了基于请求/授权的非竞争机制。

3.3　上行 DoS

DoS 攻击导致所有注册激活的用户拥有的标准服务失效和潜在网络不连通, 如果网络设备遭到攻击, 只要一个本地机器遭到入侵, 服务质量就会严重下降。一般所谓的攻击, 是通过消耗目标系统中共享的可用带宽和网络资源来实施的, 过载一些紧张的部件, 多数情况下是无限的任务。从用户的角度看, 这就会导致合法用户无法访问和(或) 服务质量(QoS) 下降。标准的 DoS 攻击有很多种实施方式, 主要有以下三种安全威胁:

a) 消耗计算资源, 如带宽、硬盘空间或 CPU 时间;

b) 破坏系统敏感配置信息, 如路由信息、LLID、MAC 地址、VLAN 标签等;

c) 破坏物理层网络连通性, 如用强激光信号使上行信道溢出, 从而阻止合法用户的有用信息的传输。

PON 网络尤其是 EPON 中最简单的 DoS 攻击, 是简单地破坏网络连通性。在特殊情况(EPON 是 P2M 结构) 下, 它受上行信道中适当波长传输的强激光信号源限制(图 4) , 与选择的上行传输窗口一致。

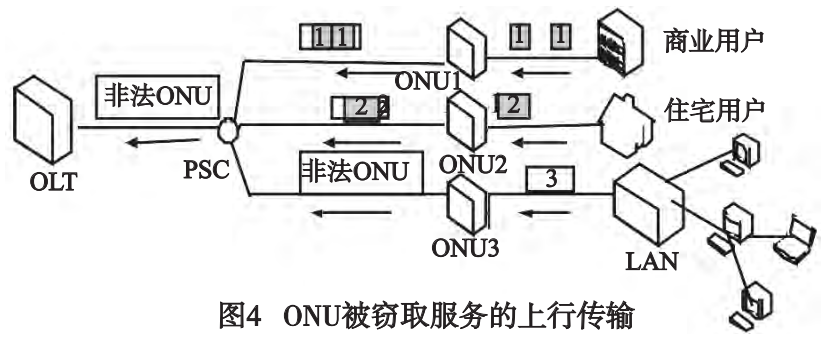

图4　ONU被窃取服务的上行传输

这可能会导致网络上行信道锁定(lock down) ; 而且, 由于激活维持(keep alive) 机制的运行, 会导致系统重启, 使得资源被黑客入侵, 破坏精心制作的安全机制。这种攻击下, 该系统要得到保护只有两种方式, 要么降低整个 PON 系统效率(如用被动式信号功率测量技术) , 探测和处理 DoS 来源; 要么上行的传输通道动态切换, 以避免传输被干扰。前者的地址方案是可行的, 通常可用于一个 EPON 系统下的 DoS 攻击, 而后者则是相当难以实施, 主要是由于安置在 ONU 中的激光源波长是固定的, 以及缺乏适当的信令协议。总之, 这样一个简单的 DoS 攻击, 对网络结构、QoS 以及数据的安全性有非常严重和破坏性的影响,

EPON 具有完全被动的网络结构, 在 ONU 与 OLT 之间没有一个积极的信号路由器, 各种依靠特定系统功能(如中断路由表等) 的 DoS 攻击不一定能发生。仅扰乱系统敏感的数据——包括 MAC 和 LLID 地址, 是有可能的; 伪造假冒 REPORT MPCP DU 请求过大的带宽, 造成设计拙劣的 DBA 算法给恶意的 ONU 分配大量可用的系统资源, 而其余的合法用户却“挨饿”。实施一个 ONU 频繁更换 MAC 地址, 可能会引起中央的突发控制器很快用尽可用的 MAC 地址, 而拒绝为任何新接入的合法 ONU 注册。同样地, 可以在 LLID 层伪造。LLID 地址空间是有限的, 因此恶意的 ONU 运行窜改过的注册策略可注册几千个 LLID, 直到中央 OLT 控制器再次耗尽地址空间, 开始拒绝为合法用户服务。针对这种攻击(基于 MAC 和 LLID) , 可能的对策包括用户敏感数据加密(混杂模式下 LLID/MAC 域的传输) 与连接认证[10,11] 以及利用到期(timeout) 活动。Time-out 最先被 IEEE 802.3 ah 标准化组织采用。一个预先定义的时间段内, 若 ONU 不能响应 keep alive 机制, 就会自动注销它注册的 MAC/LLID。这样可防止不太复杂的系统级 DoS, 即单个恶意 ONU 经常变化 LLID/MAC 的数据的情况。但是最近推出的分布式 DoS(DDoS) 攻击, 也是单个网络的 DoS 攻击的简单修改, 可能会证明 time-out 活动对系统级安全无效。

只要恶意用户将 ONU 的工作模式设置成混杂模式, 就可

以自由地访问下行数据传输通道,可以跟踪目标 MAC/LLID 和 OLT 之间的所有数据流,很容易给当前修改过 ONU 分配一系列 LLID 和 MAC 地址,并追踪 EPON 的 keep alive 机制的运行情况。当 keep alive 的 GATE MPCP DU 传递给这样一个虚 ONU,黑客只需要根据目标行为,用零/最大带宽请求来哄骗合法的 GATE MPCP DU 即可。以 MAC/LLID 地址空间溢出为目标,传输一个零尺寸 REPORT,迫使 OLT 跟踪给定 ONU,而最大尺寸的 REPORT 又为这样一个虚设备请求带宽,从而限制了合法用户使用资源。有趣的是,其他 PON 系统也不能对这种攻击免疫,无论是 GPON 还是较早的 Apon/Bpon 系统,均会发生这种攻击。据称在这一点上,只有适当设计的加密和认证机制保护系统敏感数据(如 EPON 中 MAC 及 LLID 地址),才能限制这种恶意攻击的活动机会。

4 EPON 中的伪装和窃取服务

一般来说,当一个用户企图冒充另一个合法的网络用户(即伪装),伪造他的数字签名,企图使用不要冒充者账户付费的或冒充者没有第一优先权的网络资源(带宽、访问特殊的付费服务等),窃取服务(ToS)攻击就发生了。网络结构上的初始伪装攻击是基于被动监测,在此期间,恶意用户收集目标设备(ONU)信息,包括 LLID 的数目、MAC 地址、RRT 等。这些收集到的信息是用来对恶意 ONU 进行伪装的,主要通过操纵每个传输数据帧(MAC 及 LLID 地址)中的系统敏感数据,如图 5 所示。攻击者用目标设备的 LLID、前导码 CRC 码以及 MAC 地址域(为明确起见,没画在图上)的值替代他自己的 EPON 硬件(ONU)自动生成的相应值,从而使他的帧看起来好像来自不同的 ONU。这样很容易蒙混过关,传递了大量的上行数据不被起诉,因为所产生的传输费用将被计算在另一个使用的目标 ONU 的用户(或用户组)的账户上,而恶意用户却享受较低的介质访问费用。

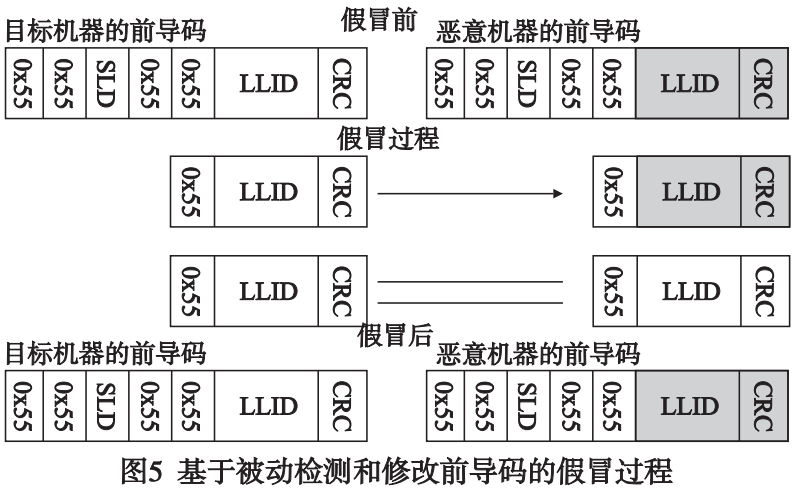

图5 基于被动检测和修改前导码的假冒过程

这里必须指出,在每个 ONU 注册阶段,OLT 为 ONU 提供了一个数字水印的身份,它用于随后的双边传输(上行/下行通道),并在传送数据帧时由 ONU 和 OLT 插入。然而,用纯文本格式传递重要和安全敏感型的数据,为实施伪装攻击提供了很好的机会;接着一般是 ToS,恶意用户只要在上行传输时简单伪造自己的 LLID,即以另一个 ONU 的合法 LLID 来替换自己的 LLID 即可。如果用户足够了解 EPON 系统的硬件,这一步只是禁用 LLID 过滤,需要被动监察流量,如上所述。当然,不能在一个随机的时刻伪造 LLID 和转发帧,因为上行通道是被分成各个时间间隙的,且访问时间是由中央 OLT 控制器严格监督。因而,这样的伪装者也一定能被动监测所有下行流量,对 LLID 过滤传入数据流。具体来说,跟踪和解码在预定传输窗口携带信息的 GATE MPCP DU,尤其是其时间和大小。ToS 和伪装攻击一旦正在进行,通常难以察觉,因为恶意的用户被认为是一个合法的,这种情况下 EPON 系统不能正确识别安全威胁。

5 EPON 中的鉴定与数据保密

就网络结构和介质访问而言,EPON 是非常开放的。一个新的 ONU(用户)是在发现过程自动接入的,除非预先确定 ONU(LLID)个数耗尽或没有新设备可进入该系统。但是,这种开放的运行模式使未经授权的用户可以获取系统资源,只需简单地开启他的 ONU,并连接到一个理论上不活跃的预留区(如预留下来为以后的配置用,或作为备份区,或不在配置时间内组装)。在这样一个开放的系统结构中,用户认证是一个必要的功能。通常认为 ONU 必须加以认证,但有必要考虑每个 ONU 可能拥有一定数量的 LLID,用户其实是与 ISP 签署了 SLA(service-level agreement,服务等级协议)的,协议清楚定义了使用的 LLID(和相应的流量等级)的数目。分配给特定 ONU 的 LLID 的实际数目,一般要考虑正常流量开销和 QoS/SLA 两方面的要求。正常流量开销受增加的逻辑实体影响,而单 ONU 单 LLID 模式受标准(IEEE 802.3 2005-Clause 64.1.1)支持。单 ONU 多 LLID 模式也由一些芯片厂商提供,这扩充了现有的标准规格,并提供了多端口 ONU 的模块。对于非标准兼容 ONU 单元多逻辑实体,实际分配的 LLID 数量通常是 3 ~ 8,具体取决于所支持的流量等级的数目、它们的映射机制以及提供给终端用户的 QoS 的粒度。

尽管如此,可以预测,只要增加的传输开销可缓解,下一代的 EPON 设备可能会为每个接入用户提供三重 LLID 支持。而提高数据业务的信道带宽的可用性或修改克服 MPCP 的低效性可缓解传输开销。具体情况可能有所不同,如单个用户可能只被分配一个 LLID。在这两种情况下,认证数据在每个 LLID 基础上发送,而不是作为一个整实体的 ONU。这可以防止 ONU 的误用,而单个的设备是由合法用户和恶意用户共享的,针对后者的服务断绝也影响前者。

用于 EPON 的各种形式的认证协议被提出来[10~14],但一般要求大幅度地修改,以规范 MPCPDU 流(尤其是在发现过程),以及有选择地使用安全认证服务器形式的第三方服务(如 RADIUS)。这样的解决方案虽然提供高水平的认证,但却使网络的整体结构复杂,且与现行 MPCP 规格不兼容。在不久的将来,对所说的标准进行明显的修改很困难。因此需要其他形式的 ONU/LLID 级认证,即利用固有的 EPON 系统中的信息进行数据完整性验证的新方法,以及(最有可能)对所有 MPCP 信息进行强有效载荷加密或其他机制,有待于进一步研究。

6 结束语

EPON 是目前接入网研究的热点,2009 年下半年,10 G EPON 的标准就要正式出台了,而安全问题是其关键技术之一,安全问题的解决影响着商用的进程。本文结合具体的 EPON 结构和原理,全面分析了 EPON 系统中各种安全攻击(从简单的被动监测到 DoS,再到伪装和 ToS)实施的原理、过程及其危害性,并提出了相应的对策,包括鉴定、安全封装、加密、入侵检测、利用到期活动等,为进一步研究 EPON 安全问题,开发灵活、高效、低价的安全方案,推动 EPON 商用进程奠定了基础。

(下转第 725 页)

的或不可信的流量在经过一段时间后会被送入到 IPS 中进行检测, 这样就意味着没有永远可信或恶意的 IP 存在。

3) 入侵数据库模块

该模块用于保存检测引擎的数据结果, 以用于建立和维护入侵威胁度所需信息。其中的内容分为两部分: a) 入侵信息, 包含 IP 地址、入侵方式、入侵的危险等级、频率(这里可以依据 IPS 工具自身的日志分析系统) ; b) 正常访问的信息, 只包含 IP 和频率。每产生一次正常访问, 该 IP 的威胁度便有一定程度的降低。

3　系统评测

本文研究的目标是消除 IPS 瓶颈, 提高分流系统的可靠性和适用性。下面在理论上简单验证系统的性能。

假设服务器性能是 IPS 检测性能的 k 倍, 原有 IPS 检测漏报率是 m, 威胁裁决系统的错误率为 n, 其值可以随威胁区间改变。

a) 当网络流量远大于服务器处理能力时, 在原有 IPS 工作的情况下, 服务器的利用率为 $1/k$, 漏报率为 m。在本系统工作以后服务器利用率为 100%, 漏报率在此处随着威胁区间和网络流量的变化而变化。在网络流量不断变大的同时, 威胁区间向威胁度减小的方向移动, 同时漏报率不断降低, 最后达到极限值 m/k。

b) 当网络流量低于服务器能力而高于 IPS 处理能力时, 在原有 IPS 下, 服务器利用率为 $1/k$, 漏报率为 m。在本系统下工作的服务器性能利用率和具体流量及威胁区间有关, 该值大于 $1/k$; 漏报率和威胁区间及威胁评测系统产生的错误率有关, 在 $n > m$ 的情况下, 其值最大不超过 $n \cdot (k - 1)/k + m/k$。

c) 当网络流量低于 IPS 处理能力时, 本系统工作于正常模式下, 与原有 IPS 性能相同。

由上述情况可知, 本系统可以有效提高服务器的利用率, 同时在大流量情况下改善入侵检测性能, 减少漏报率。在部分情况下, 本系统可能会导致漏报率提高, 但是其漏报率是可控制的, 通过改进算法减少威胁评测系统的错误率 n 和调整威胁区间, 可对漏报率进行调整, 将其控制在可接受的范围内。

4　结束语

加入了分流系统以后, 服务器的性能不再受缚于 IPS 的瓶颈, 而分流系统的有效性很大程度上取决于分流的标准。如果漏报率太大, 分流系统就无法适用于对安全性有着较高要求的场合。本文将威胁排序方法应用于分流技术上, 提高了分流系统的适用范围, 而且本文中各个模块均可在软件平台上实现, 无须特殊的硬件系统, 所以适用性较广。然而本系统仍然存在一些不足, 在威胁度排序算法上, 层次分析法在目标较多时计算比较复杂, 在实时环境下对计算机性能有一定的要求, 下一步希望能够对算法进行改进, 使之能够更好地适应本系统要求。由于研究时间较短, 尚未对系统进行各种网络环境下的详尽测试, 本系统目前还不能适用于诸如银行、保险等对安全性能要求极高的环境。下一步将对系统的各项参数进行详尽测试调整, 进一步提高分流的准确性, 使之满足对安全要求较高的情况。

参考文献:

[1] ONZALEA J M, PAXSON V, WEAVER N. Shunting: a hardware/software architecture for flexible, high-performance network intrusion preventionp[C] //Proc of the 14th ACM Conference on Computer and Communications Security. New York: ACM Press, 2007: 139-149.

[2] CLARK C, LEE W, SCHIMME L D, *et al*. A hardware platform for network intrusion detection and prevention[C] //Proc of the 3rd Workshop on Network Processors and Applications. 2004.

[3] CROVELLA M. Performance evaluation with heavy tailed distributions[C] //Proc of the 7th International Workshop on Job Scheduling Strategies for Parallel Processing, London: Springer-Verlag, 2001: 1-10.

[4] SATTY T L. The analytic hierarchy process[M]. New York: McGraw-Hill Professional Publishing, 1980.

[5] 王莲芬, 许树柏. 层次分析法引论[M]. 北京: 中国人民大学出版社, 1990.

[6] 王应明. 判断矩阵排序方法综述[J]. 决策与决策支持系统, 1995, 5(3): 107-114.

[7] YAGER R R. On ordered weighted averaging aggregation operators in multicriteria decision making[J]. IEEE Trans on Systems, Man and Cybernetics, 1988, 18(1): 183-190.

(上接第 722 页)

参考文献:

[1] EEE. 802.3[S/OL]. [2005]. http://en.wikipedia.org/wiki/IEEE.802.3.

[2] HAJDUZENIA M, da SILVA H J A, MONTEIRO P P. EPON versus APON and GPON: a detailed performance comparison[J]. Journal of Optical Networking, 2006, 5(4): 298-319.

[3] KRAMER G. Ethernet passive optical networks[M]. New York: McGraw-Hill Professional Publishing, 2005.

[4] KRAMER G, MUKHERJEE B, MAISLOS A. Multiprotocol over DWDM: building the next generation optical Internet: ethernet passive optical networks[M]. Hoboken, NJ: Wiley, 2003.

[5] CHAE C J, WONG E, TUCKER R S. Optical CSMA/CD media access scheme for Ethernet over passive optical network[J]. IEEE Photonics Technology Letters, 2002, 14(5): 711-713.

[6] KRAMER G, MUKHERJEE B, PESAVENTO G. Interleaved polling with adaptive cycle time (IPACT): a dynamic bandwidth distribution scheme in an optical access network[J]. Photonic Network Communications, 2002, 4(1): 89-107.

[7] KRAMER G, MUKHERJEE B, PESAVENTO G. IPACT: a dynamic protocol for an Ethernet PON (EPON)[J]. IEEE Communications Magazine, 2002, 40(2): 74-80.

[8] KRAMER G, BANERJEE A, SINGHAL N K, *et al*. Fair queuing with service envelopes (FQSE): a cousin-fair hierarchical scheduler for subscriber access networks[J]. IEEE Journal on Selected Areas in Communicatiions, 2004, 22(8): 1497-1513.

[9] MA Mao-de, ZHU Yong-qing, CHENG T H. A bandwidth guaranteed polling MAC protocol for ethernet passive optical networks[C] //Proc of the 22nd Annual Joint Conference on IEEE Computer and Communications Societies. 2003: 22-31.

[10] MURAKAMI K, FUJIMOTO Y, YOSHIHARA O. Authentication and encryption in EPON[R/OL]. (2002-07). http://www.ieee802.org.13/efm/public/ju/02/p2mp/murakami_p2mp_1_0702.

[11] KIM J. Authentication and privacy in EPON[R/OL]. (2002-07). http://www.ieee802.org/3/efm/public/julo2/p2mp/kim_jin_p2mp_3_0702.pdf.

[12] HARAN O. Ethernet PON: security considerations[R/OL]. (2001-05). http://www.ieee802.org/3/efm/public/may01/haran_1_0501.pdf.

[13] ROMASCANU D, RIBEIRO C. Security aspects of the OAM protocol for EFM[R/OL]. (2002-01). http://www.ieee802.org/3/efm/public/jan02/romascanu_1_0102.pdf.

[14] GUMMALLA A, RIBEIRO C, COOK C, *et al*. Security threats and mechanisms[R/OL]. (2001-09). http://www.ieee802.org/3/efm/public/sep01/haran_1_0901.pdf.