基于状态机的流媒体入侵检测研究

刘 焱 钟国辉 刘 玉 王芙蓉
(华中科技大学电子信息与工程系 武汉 430074)

摘 要 提出了一种针对流媒体的入侵检测技术。对基于RTSP协议的流媒体应用经常遭受的诸如SETUP泛洪攻击、会话截取攻击、恶意结束流媒体会话攻击和恶意RTP攻击进行了建模。在状态迁移分析和应用层会话管理技术的基础上,利用已有的进攻模型,进行入侵检测。该技术可以有效检测上述攻击。对系统的入侵检测性能进行了建模,定量分析了该入侵检测系统的性能。分析表明,该系统有很短的入侵检测延时。

关键词 流媒体,入侵检测系统,实时流协议,状态迁移分析
中图法分类号 TP393 **文献标识码** A

Stream Media Intrusion Detection through Interacting Protocol State Machines

LIU Yan ZHONG Guo-hui LIU Yu WANG Fu-rong
(Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract This paper proposed a novel model to cope with these attacks such as SETUP flooding, session intercepting, malicious terminating stream media session and RTP assorting in stream media application based on RTSP protocol. The analysis in this paper was discussed in a particular assorting model in which the technology RTSPSTAT (RTSP Network State Transition Analysis Tool) was proposed based on state transmission analyzing and session management in application layer. In addition, the performance of this new model was quantitatively evaluated. The experiment result data show the processing method works well, specially characterized by fairly short delay of intruding detection.

Keywords Streaming media, IDS, RTSP, STAT

1 引言

基于RTSP(Real Time Streaming Protocol)[1]协议的流媒体应用日益流行。在与其他网络应用共享网络资源的同时,流媒体应用也同样遭受着各种网络攻击的侵扰。本文结合流媒体通信的特点,提出了一种基于状态分析技术的流媒体入侵检测技术——RTSPSTAT (RTSP Network State Transition Analysis Tool)。

2 相关工作

G. Vigna等人、Y. Wu等人、H. Sengar等人所做的工作与我们的工作比较接近,都是将STAT(State Transition Analysis Tool)[2]应用到网络入侵检测领域。G. Vigna等人首先提出了NetSTAT (Network State Transition Analysis Tool),将应用于主机入侵检测的STAT技术应用到网络环境[3]。随后G. Vigna等人又将STAT应用到Web的入侵检测,提出了WebSTAT (Web State Transition Analysis Tool)[4]。WebSTAT综合分析来自网络的数据流、Web服务器操作系统的信息以及服务器日志内容,判断是否发生了针对Web的攻击。Y. Wu等人和H. Sengar等人将该技术应用到VOIP的入侵检测。Y. Wu等人提出了SCIDIVE(Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments)[5],他们的主要贡献是将网络数据流按照会话区分成不同的组,将SIP会话与其对应的RTP会话关联起来分析。H. Sengar等人[6]的主要工作是使用EFSM(Extended Finite State Machine)描述了各种针对SIP的攻击模型,并且给出了基于STAT技术的VOIP入侵检测系统对呼叫建立以及流媒体传输的影响。L. Gaspary等人主要是引入SNMP,将STAT应用到分布式系统的入侵检测[8]。

3 RTSPSTAT框架

RTSPSTAT架构主要由协议识别模块、应用层会话管理模块、攻击模型模块、攻击分析模块组成,如图1所示。协议识别模块将网络驱动截获的数据报文首先按照五元组:$v=\langle src_ip, src_port, protocol, dst_ip, dst_port\rangle$区分成不同的向量,然后将属于同一应用层协议的向量关联起来,形成一个应用层会话。比如RTSP协议会创建一个RTP连接,用于传输数据,协议识别模块就将RTSP向量V_{RTSP}和RTP向量V_{RTP}关联起来,构成一个应用层会话$session=\langle V_{RTSP}, V_{RTP}\rangle$,同时应用层会话管理模块还会为该会话记录必要的信息提供定时器等资源;攻击模型模块记录了常见的攻击模型;攻击分析

到稿日期:2008-06-02 本文受国家自然科学基金(项目批准号:60502023)资助。
刘 焱 博士研究生,主要研究方向为软交换和信息安全;钟国辉 博士,讲师,主要研究方向为网络安全和嵌入式系统,E-mail:duoergun0729@smail.hust.edu.cn;刘 玉 博士,教授,主要研究方向为网络安全和嵌入式系统;王芙蓉 博士生导师,主要研究方向为软交换和信息安全。

模块综合分析应用层会话管理模块和攻击分析模块的信息，判断是否发生了入侵。与传统的基于五元组向量 v 的会话相比，基于应用层的会话更能反映用户的行为特征，更利于深入分析用户行为。

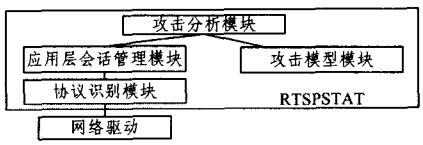

图 1　RTSPSTAT 框架

4　入侵模型

约定服务器特指 RTSP 服务器，客户端特指 RTSP 客户端。

4.1　SETUP 泛洪攻击

当服务器接收到客户端的 SETUP 请求后，会为该客户端分配一定的系统资源。攻击者通过构造大量的 SETUP 报文，使服务器的资源枯竭，无法为合法用户提供服务。由于流媒体通信需要消耗大量的资源，服务器必须为每个客户端预留足够的资源，因此 SETUP 攻击比简单的 SYN 攻击更加有效。

4.2　会话截取攻击

RTSP 协议利用 Session 字段标识和管理 RTSP 会话，该字段由服务器统一分配。攻击者获取到某个合法的 Session 后，就可以通过构造报文，伪装成合法用户，拥有合法用户的所有权限，访问服务器上的资源。

4.3　恶意结束流媒体会话攻击

如图 2 所示，服务器通过 TEARDOWN 消息告知客户端结束本次流媒体会话。攻击者在监听流媒体会话的基础上，可以通过构造源地址把服务器的 TEARDOWN 消息发往客户端，结束流媒体会话，使客户端停止接受流媒体数据。

图 2　恶意结束流媒体会话

4.4　恶意 RTP 攻击

RTP[7] 使用序列号(Sequence Number)和时间戳(Timestamp)对分组进行排序和正确回放，通过同步源标识(SSRC)区分不同的流媒体源。攻击者截取到 RTP 的 SSRC，构造具有相同 SSRC 和陡增的序列号或时间戳的 RTP 报文，扰乱客户端对流媒体的回放。

5　检测模型

5.1　SETUP 泛洪攻击

服务器和客户端建立 TCP 连接后，RTSP 会话进入初始状态。当客户端发送 SETUP 报文时，系统创建溢出时间为 T 的定时器 T1，同时初始化计数器 count，统计来自同一地址的客户端发送的 SETUP 报文的个数。由于网络的影响，可能会造成客户端的 SETUP 报文的超时重传，因此在时间 T 内发送 N 个 SETUP 报文被认为是正常情况。当发现在时间 T 内收到来自客户端的 SETUP 报文超过 N 时，认为系统遭受了攻击。其中 T 和 N 是可以配置的，通常 N 等于客户端支持的重传 SETUP 报文的最大个数。图 3 给出 SETUP 泛洪检测模型。

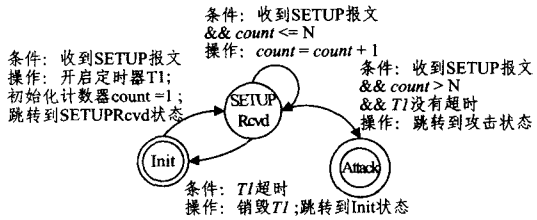

图 3　SETUP 泛洪检测模型

5.2　会话截取攻击

图 4 给出会计截取攻击检测模型。

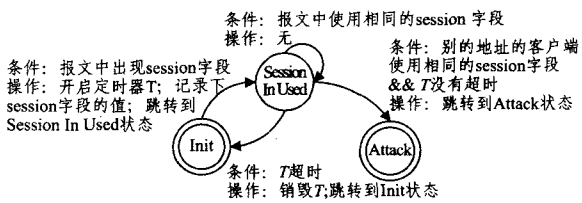

图 4　会话截取攻击检测模型

当客户端与服务器建立连接后，服务器为该客户端分配一个全局唯一的会话标识，即 session 字段记录的值。当发现使用 session 字段时，系统创建溢出时间为 T 的定时器 $T2$，同时记录下该会话标识。当在 T 溢出之前检测到别的地址的客户端使用相同的会话标识时，认为该会话标识被截取了，发生了会话截取攻击。

5.3　恶意结束流媒体会话攻击

图 5 给出恶意结束流媒体会话攻击检测模型。

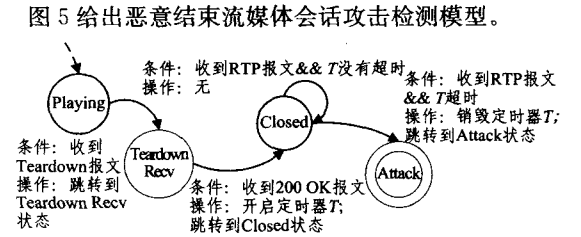

图 5　恶意结束流媒体会话攻击检测模型

当收到 teardown 报文后，服务器和客户端将结束这次 RTSP 会话，停止流媒体的传输。由于网络的影响，客户端收到 teardown 报文后，还可能收到来自服务器的 RTP 报文。设定一个时间阀值 $T3$，认为 $T3$ 内收到 RTP 报文属于正常情况，反之即遭受了恶意结束流媒体会话攻击。

5.4　恶意 RTP 攻击

图 6 给出恶意 RTP 攻击检测模型。

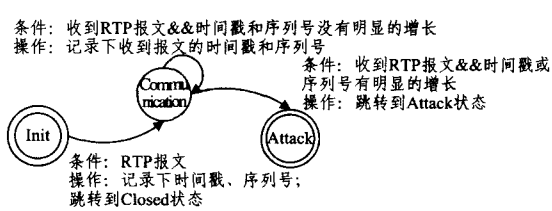

图 6　恶意 RTP 攻击检测模型

恶意 RTP 攻击主要是利用陡增的序列号或时间戳破坏

客户端对流媒体的回放。通过检查序列号或时间戳是否存在陡增或骤减，可以检测是否遭受到了恶意 RTP 攻击。

6 性能分析

流媒体对时延十分敏感，所以我们主要从检测延时的角度衡量系统的性能。所谓的检测延时 D 即系统被入侵到发现系统被入侵之间的时间差。我们结合最常见的 SETUP 泛洪攻击来分析基于状态的入侵检测系统的性能。

如图 7 所示，客户端在 0 时刻发送第一个 SETUP 报文，服务器在 t_1 时刻接受到该报文，入侵检测系统初始化计数器为 1 并开启超时时间为 T 的定时器。当服务器在时间 T 内收到第 $N+1$ 个 SETUP 报文时，系统检测出发生了 SETUP 泛洪入侵。

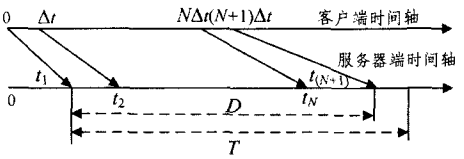

图 7 SETUP 泛洪检测模型的检测延时

检测延时 $D=t_{(N+1)}-t_1$，假定客户端每隔 Δt 发送一个 SETUP 报文，第 i 个报文（$i=1,2\cdots,N+1$）在网络中的延时 d_i 互相独立，并且服从 $U[0,\Delta t]$ 分布，即在 $[0,\Delta t]$ 范围内服从均匀分布，$Ed_i=\frac{1}{2}\Delta t$

$$t_{(N+1)}=\sum_{i=1}^{N+1}(\Delta t+di)=(N+1)\Delta t+\sum_{i=1}^{N+1}(di)$$

$$D=t_{(N+1)}-t_1=N\Delta t+\sum_{i=2}^{N+1}(di)$$

检测延时 D 的期望为

$$ED=E(N\Delta t+\sum_{i=2}^{N+1}(di))=N\Delta t+\sum_{i=2}^{N+1}(Edi)=\frac{3}{2}N\Delta t$$

通常客户端允许重传的个数为 6，N 取 6，Δt 很小，通常为毫秒级，取 $\Delta t=10$ms，所以检测延时 D 的期望的典型值为 90ms。

结束语 本文针对流媒体经常遭受的诸如 SETUP 泛洪攻击、会话截取攻击、TEARDOWN 恶意攻击、RTP 恶意攻击，建立了相应的攻击模型，在状态迁移分析和应用层会话管理技术的基础上提出了 RTSPSTAT 技术，并定量分析了其性能。

未来的工作主要是进一步丰富入侵检测模型，提高系统的实用性。

参 考 文 献

[1] Schulzrinne H, Lanphier R, Rao A, et al. RFC 2326, Real Time Streaming Protocol (RTSP). IETF Network Working Group, 1998

[2] Vigna G, Eckmann S T, Kemmerer R A. The STAT tool suite [C]// DARPA Information Survivability Conference and Exposition(DISCEX '00). Proceedings. IEEE, 2000: 46-55

[3] Vigna G, Kemmerer R. NetSTAT: A Network-based Intrusion Detection Approach [C] // Proceedings of the 14th Annual. IEEE, 1998: 25-34

[4] Vigna G, Robertson W, Kher V, et al. A Stateful Intrusion Detection System for World-Wide Web Servers[C]// Computer Security Applications Conference, 2003. Proceedings. 19th Annual. IEEE, 2003: 34-43

[5] Wu Y, Bagchi S, Garg S, et al. SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments. Dependable Systems and Networks[C] // 2004 International Conference on. IEEE, 2004: 433-442

[6] Sengar H, Wijesekera D, Wang Haining. VOIP Intrusion Detection Through Interacting Protocol State Machines. Dependable Systems and Networks. IEEE, 2006: 393-402

[7] Schulzrinne H, Casner S, Frederick R, et al. RFC 1889, RTP: A Transport Protocol for Real-Time Applications. IETF Network Working Group, 1996

[8] Gaspary L P, Sanchez R N, Antunes D W, et al. SNMP-based platform for distributed stateful intrusion detection in enterprise networks[J]. Selected Areas in Communications, IEEE Journal, 2005, 23(10): 1973-1982

（上接第 81 页）

参 考 文 献

[1] Zander J. Performance of optimum transmitter power control in cellular radio systems [J]. IEEE Transaction on Vehicular Technology, 1992, 41

[2] Manji S, Zhuang W. Power control and capacity analysis for a packetized indoor multimedia DS-CDMA network [J]. IEEE Transaction on Vehicular Technology, 2000, 49

[3] Kelly F P, Maullo A, Tan D. Rate control for communication networks: shadow prices, proportional fairness and stability [J]. J. Oper. Res. Soc., 1998, 49(3): 237-252

[4] Low S H, Lapsley D E. Optimization flow control, I: basic algorithm and convergence [J]. IEEE/ACM Transaction on Networking, 1999, 7(6): 861-875

[5] Low S H. A duality model of tcp flow controls [C]// ITC Specialist Seminar on IP Traffic Measurement, Modeling and Management. 2000

[6] Chen Lijun, Low S H, Chiang Mung, et al. Cross-layer congestion control, routing and scheduling design in ad hoc wireless network[C]// Proc. IEEE INFOCOM. 2006

[7] Chiang M. Balancing supply and demand of bandwidth in wireless cellular networks: utility maximization over powers and rates [C]// Proc. IEEE INFOCOM. Hong Kong, China, March 2004

[8] Nama H, Chiang M, Mandayam N. Utility-lifetime tradeoff in self-regulation wireless sensor networks: a cross-layer design approach [C]// IEEE ICC. 2006

[9] Nama H, Chiang M, Mandayam N. Optimal utility-lifetime tradeoff in wireless sensor network: Characterization and distributed solutions [J]. IEEE Transaction on Wireless Communications. 2007

[10] Liao Shengbin, Liu Wei, Ding Yi, et al. Distributed Optimization of Sensor Networks Based on NUM [C]// Glasgow, Scotland, ICC. 2007

[11] Sadagopan N, Singh M, Krishnamachari B. Decentralized utility-based sensor network design [J]. Mobile Networks and Applications, 2006, 11: 341-350