Satellite Network Protection against PEP-Related Vulnerabilities

F. BELLI[a], M. LUGLIO[a] , C. ROSETI[a,1]

Abstract. This paper deals with security for heterogeneous and inter-operable communication networks including a satellite segment. Integration of different networks enhances sustainable applications but specific vulnerabilities must be faced up too. INTERSECTION project[2] is aimed to both design and implement an Intrusion Detection System (IDS) for the detention of anomalous events in the interconnected networks attributable to security attacks. The present work is focused on the application of INTERSECTION IDS on the target scenario, where the presence of Proxy Enhancing Proxies (PEPs) at the edges of satellite links leads to the twofold effect of improving TCP performance but also increasing a PEP-related vulnerability due to the violation of the end-to-end semantic of TCP. Then, the paper addresses the above mentioned issue through the realization of a test bed including a real geostationary satellite link operated by Telespazio.

Keywords. IDS, PEP, TCP

Introduction

One of the major trends in the commercial communications market is the adoption of wireless technology. In addition, the need to exchange information anywhere and anytime requires the adoption of different inter-operable and cooperative technologies. In this context, geostationary (GEO) satellite systems are particularly suited to support large-scale broadband applications. As a drawback, in most of cases traditional TCP/IP stack and related paradigms [1] result in poor performance since assumptions considered in the protocol design donôt match with the actual environment. Scientific literature and commercial products have largely addressed this issue proposing a vast gamut of protocol and architectural solutions [2][3][4].

A common baseline envisages the use of Performance Enhancing Proxies (PEPs) at the edge of satellite links with the main scope to ñaccelerateò TCP over satellite [2]. PEP is mainly based on a splitting architecture, which divides end-to-end connections into multiple sub-connections, each one adopting a transport protocol suited to the link characteristics (i.e. delay, bandwidth, BER). Over the satellite link, ad-hoc transport protocols usually replace standard TCP.

Although performance improvement is significant, PEP-based architecture is intrinsically vulnerable due to the violation of the TCP end-to-end semantic. A PEP

[a] Centro Radioelettrico Sperimentale Marconi CRESM, Tor Vergata research unit, via del Politecnico 1, 00133, Rome.

[1] Corresponding Author.

[2] INTERSECTION is a collaborative project co-funded by the EC in the frame of the Seventh Framework Programme under the Area 5 subprogramme: ñSecurity, Privacy and Trust in the Future Internetò.

intentional or unintentional failure (i.e. dropping of locally acknowledged packet before reaching actual destination) leads to an irreversible break of the end-to-end reliability. Security implications are straightforward since TCP can be used to provide transport services to applications with severe reliability requirements.

This vulnerability is addressed by INTERSECTION Intrusion Detection System (IDS), which has been properly tailored to detect anomalous events along interconnected networks and provide countermeasures to avoid system failure. More in detail, the overall IDS architecture envisages distributed modules for detection, modules for reaction/remediation and modules for the visualization. Target vulnerability as well as IDS will be implemented in a demonstration test bed composed of three real interconnected domains: a satellite link, which connects local networks of a mobile telecommunications provider and a telephone operator. So far, IDS has been validated on a Linux emulator platform, which reproduces the main dynamics of a DVB-RCS satellite network. This paper aims to present the main aspects of both demo scenario and IDS design.

1. Reference scenario and test bed setup

Target vulnerability can be reproduced in a communication scenario where a satellite geostationary link, operated by Telespazio (TSP), is used to interconnect a remote terrestrial LAN of Polska Telefonia Cyfrowa (PTC) with an Internet Service Provider (ISP) represented by Telefonica (TID). TID interfaces the satellite gateway, while PTC interfaces a satellite terminal. The application foresees a user in PTC network that uploads files in an FTP server installed at TID premises. A TCP connection is established to provide an end-to-end reliable byte stream. PEP agents running at the edges of the satellite link split end-to-end TCP connection, so that:

- an end-to-end TCP three-way handshake (TCP SYN flag on) is performed,
- three different sub-connections are created and managed by PEP agents,
- each PEP manages a local cache to store all the sent packets not yet acknowledged by the actual receiver.

Test bed core relies on hardware in the loop configuration where a real satellite link (Intelsat 901 @ 342° E) operating at Ku band with a channel of 600 kHz is accessed by two satellite modems. At the edges of such a satellite link, both a Satellite Gateway/Network Control Centre (satGW/NCC) and Return Channel Satellite Terminal (RCST) functionalities are emulated through Linux-based machines. The rationale is to add to satellite link features also a DVB-RCS-like access scheme. Briefly, RCST will require bandwidth for the return link on the basis of its actual needs (i.e. amount of bytes stored in the MAC queue). PEP agents are installed in both satGW/NCC and RCST machines.

2. Description of the PEP-based vulnerability

In the given communication environment, a malicious user in TID network can access PEP in front of satGW with the aim of installing a malware application that performs the task to drop a part or all TCP packets incoming from PTC network. Different

harmful effects can be caused depending on both malware implementation and application protocol:

1) loss of several packets within a connection causes continuous retransmissions, for instance after a retransmission timeout expiration, increasing transfer time;
2) packet dropping does not allow the application to successfully conclude its operations and end-system is aware of the negative transfer outcome;
3) packet dropping is transparent to applications that trusts on a successfully transfer.

The first effect is not strictly related to a classical attack, since file transfer is finally achieved although delayed and forced retransmissions require additional satellite resources. This could lead to worsen the QoS and to increase both the service costs and congestion of satellite return link, usually representing the bottleneck of the whole link. The second effect is a typical Denial of Service (DoS) attack. All TCP-based transfers fail, while traffic however crosses the satellite link. DoS implies a huge waste of satellite resources. In addition, failed transfers could be continuously reattempted. The last effect is surely the most harmful as far as the security is concerned. In fact, TCP sources (i.e. FTP clients) trust on a correct progress and completion of transfers. This may mislead user for instance to delete sent file.

This attack has a heterogeneous nature since it exploits a vulnerability of the satellite network; it is generated from ISP network and it impacts on FTP client located in a remote LAN.

3. IDS for satellite network protection

Satellite IDS exploits two types of probes based on OpenIMP [5]: the ñSYN detectorò and the ñTCP traffic analyzer. The ñSYN detectorò is installed on SatGW and has in charge to monitor all the TCP traffic in order to create an IPFIX record for every SYN/FIN exchange through satellite link. Each record includes the parameters identifying the specific connection and it is enhanced with the time information.

ñTCP traffic analyzerò probes run on the access router of all the networks interfaced to the satellite network. Such probes aim to collect statistics about TCP traffic coming from and going to the satellite network. Specifically, a TCP traffic analyzer grabs the number of transferred bytes over any active TCP connection. A time interval must be defined for such measurements. A large value allows a better measurement accuracy, but it slows down statistic updates for the attack detection matters. On the contrary, a low value could be affected by transitory traffic dynamics, as for instance unexpected traffic spikes or idle times. Therefore, a trade-off value of 10 s has been chosen as default.

All the probe records are collected by a *data broker*, which represents the first functional element of the IDS. Data broker is in charge to forward the received records to the *Detection Engine*, which implements the following detection logic:

Step 1. Compare the number of SYN records with that of FIN records coming from the SYN detector probe; if #SYN ≅ #FIN, regular operations are assumed; otherwise (#SYN - #FIN > threshold = 10) detection process moves to step 2;

Step 2. Delete <#SYN ; #FIN> pairs related to a same connection; residual SYN records will provide information on networks involved in possible attack.

Step 3. For each connection under investigation, compare the amount of bytes crossing corresponding source-destination networks; results are computed in the form of ñbyte differencesò.

So-achieved results are then forwarded to the *decision maker* that determines if, what has been detected as an anomaly can be forwarded as an attack to an external entity.

The Reaction and Remediation (*ReaRem*) subsystem involves a *Reaction Engine*, a repository of scripts used for the attack remediation, and a *Remediation Point*, which represents the network element where such scripts will be run. Specifically, when an attack is detected (decision maker issues a trigger), the Reaction Engine downloads the appropriate script from its repository to stop PEP misbehavior. This script, executed in the Remediation Points/PEPs, performs a procedure aimed to temporary disable PEP involved in the attack in order to recover correct settings: delete of the malware and reset PEP routing tables.

The overall scheme of the proposed test bed scenario is sketched in the Figure 1.

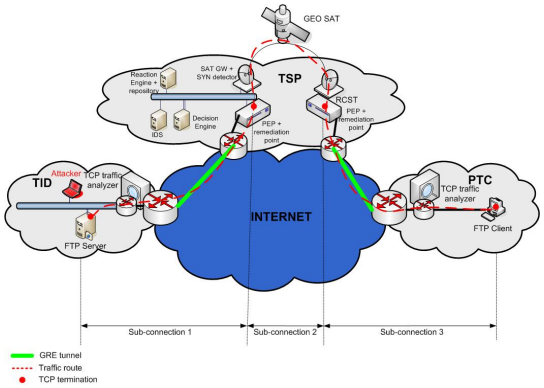

Figure 1. Test bed scenario

4. Conclusions

This paper presents the design of an IDS tailored to security issues coming from the adoption of PEP at the edges of the satellite link. PEP is fundamental to improve TCP performance over satellite, but it is intrinsically vulnerable due to the violation of the TCP end-to-end-paradigm. The proposed IDS addresses PEP-related vulnerability with the aim to make possible the combination of optimized performance and network protection, as requested for the future Internet. Overall system will be tested on a test bed including a real satellite link operated by TSP.

References

[1] W. Stevens, ñTCP/IP Illustrated. Vol.1ò, Ed. Addison Wesley, 1994.

[2] J. Border, M. Kojo, J. Griner, G. Montenegro, and Z. Shelby. Performance enhancing proxies intended to mitigate link-related degradations. RFC 3135, IETF, June 2001.

[3] C. Partridge, T. J. Shepard, ñTCP/IP Performance over Satellite Links,ò IEEE Network, September October 1997, pp. 44-49.

[4] C. Caini, R. Firrincieli, M. Marchese, T. De Cola, M. Luglio, C. Roseti, N. Celandroni, F. Portontì, Transport Layer Protocols and Architectures for Advanced Satellite Networks, International Journal of Satellite Communications and Networking, Vol. 25, Oct. 2007, pp. 1-26, DOI:10.1002/sat.855.

[5] http://openimp.sourceforge.net