

# Using Decoys to Prevent Attacks on IPTV Systems in the IP Multimedia Subsystem

Phillippa R. Wilson, Neco Ventura  
Department of Electrical Engineering, University of Cape Town,  
Rondebosch, Cape Town, South Africa  
{pippa, neco}@crg.ee.uct.ac.za

**Abstract**—Multimedia web servers are vulnerable to attack due to their large storage capabilities. The IP Multimedia Subsystem (IMS) is also vulnerable due to its high-speed links. Furthermore, it is difficult to detect malicious traffic in such networks. As a result, IMS-based IPTV systems are targets. Currently, there are no standardised security techniques to secure IPTV web servers. This Work-in-Progress paper discusses the current techniques used to secure web-based systems and networks, such as intrusion detection systems (IDS), firewalls and decoys. The framework proposed in this paper uses the honeynet to detect malicious traffic and secure IPTV systems.

**Index Terms**—Decoys, Honeynets, IPTV, Security

## I. INTRODUCTION

IMS-based IPTV is said to be “the way it should be” [1]. This is since the infrastructure of the IMS is able to support multi-play services while assuring a high Quality of Service to the subscriber, at a reasonable price.

However, the large storage capabilities and high bandwidth links, which are characteristic to multimedia applications like IPTV, make the systems targets for attackers [2]. History is filled with examples of exploited web-based application systems. Hackers are always looking to compromise systems or steal and abuse network resources [3]. These attacks can lead to legitimate users experiencing a noticeable degradation of services, a complete denial of services, or a large bill for services which a hacker used at their expense. For the service provider, attacks on IPTV systems may lead to a loss in revenue and a bad reputation. Therefore, ensuring the security of these IPTV multimedia systems is an essential requirement from both the subscribers and service providers’ point of view.

As the Internet grew in popularity from its introduction in the late 1960’s, its development was driven by functionality and not security. As a result, web-based security has always been an open area of research. Furthermore, as web applications continue to grow, the rate of web application attacks grows proportionally. Currently, there are no standardised security techniques specified for securing IPTV application systems in the IMS.

The authors would like to thank Telkom SA, the National Research Foundation (NRF), Technology and Human Resources for Industry Programme (THRIP), the Department of Trade and Industry (DTI), Nokia Siemens Networks and TeleSciences, for supporting this research project.

## II. RELATED WORK

Web servers provide services 24 hours a day and therefore cannot be shut down to analyse suspicious activity [4]. Attacks on IPTV systems must therefore be prevented without disturbing the normal operation of the media server.

According to Sher & Magedanz [5], the challenging security threats of web-based services are: Denial-of-Service (DoS) attacks to sabotage servers and legitimate users; unauthorised access to cause theft or fraud; message modification to cause collapse of applications and servers; and eavesdropping to steal services or gain access to confidential information.

Although encryption and digital signatures can be used to countermeasure most of these threats, not all the attacks are addressed by these techniques. Firewalls and intrusion detection systems are traditionally used to protect against the remaining attacks. Within the Internet, the DoS attack was suggested as the most challenging type of attack at this time [5]. Many works, including Khattab et al. [6] proposes a honeypot-based solution for this problem.

### A. Firewalls

Firewalls are used to control the flow of traffic between a local network and the public Internet [2]. As a result, firewalls cannot prevent against internal attacks or dial-in/dial-out attacks which bypass the firewall. Furthermore, high volumes of network traffic, which is characteristic to all multimedia applications, may overwhelm the firewall allowing malicious traffic to pass through, undetected.

### B. Intrusion Detection Systems (IDS)

IDSs are used to detect exploitations and alert system administrators. Sensors are placed at various points around the network. There are two types of IDSs: signature-based and anomaly-based. Signature-based IDSs cannot protect against unknown or new types of attacks. Anomaly-based IDSs result in a high level of false positive alerts, making quick response to attacks very difficult. Furthermore, IDSs increase the complexity of the security management problem due to the distributed nature of the sensors and the large amount of data captured and processed [2].

Due to these shortcomings, the above two techniques are not adequate on their own for securing IPTV systems in the IMS. The introduction of an additional security layer may be the solution.

### C. Decoys

The concept of decoys has been proposed in a number of works [2] [3] [4] [6] [7] to enhance network security and protect application systems. These techniques are able to

overcome the critical shortcomings of the traditional techniques discussed above. They are designed to work in conjunction with firewalls and IDSs, offering an additional layer of security.

A honeypot is a decoy system, designed to be a target for attackers. It is a resource whose value lies in it being probed, attacked or compromised by an attacker [8]. Honeypots use deception or deterrence to confuse, slow down or stop attacks [7]. It has been shown in Artail et al. [7] that the use of honeypots is effective in reducing the probability of attacks on production systems in networks. The addition of more decoys in the network will decrease this probability even further.

The honeynet is a network of multiple high-interaction honeypots creating the illusion of a production network [8]. This is shown in figure 1. Each honeypot in the honeynet is capable of offering real services to an attacker. As a result, the attacker will be oblivious to the honeynet's operation and will allow the honeynet to capture extensive information on his/her activity. The honeywall is invisible to attackers and mitigates the risk of an attacker causing harm to production systems from within the honeynet.

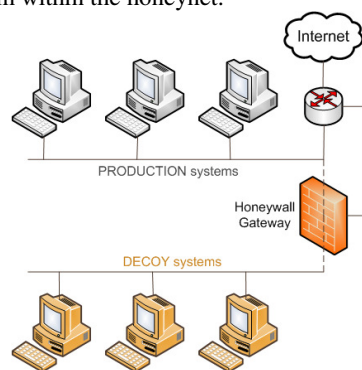


Fig. 1. The honeynet architecture.

### III. RESEARCH GOALS

A security architecture is required to overcome the shortcomings of firewalls and IDSs and to incorporate the benefits of layered security. This architecture must secure IPTV multimedia application systems, on large networks such as the IMS, against malicious traffic exploits. This must be done without a negative effect on the user's quality of experience.

Other requirements of the proposed architecture include detection of any type of attack, quick response to threats, real-time analysis for the real-time application, scalable to large networks and compatible with the IMS and IPTV network architectures.

### IV. PROPOSED SECURITY ARCHITECTURE

Since a honeynet is designed to disguise itself as a production network and be targeted by attackers, it is necessary for the decoy systems to be located where an attacker would expect to find the real systems. As a result, the honeynet should be located in the application layer of the IMS, where the real IPTV web server and databases are located.

The production systems in the honeynet are the real IPTV systems, while the decoy systems are running the same operating systems and offer the same services as the real

ones. The honeywall isolates the decoy systems from the rest of the network and is invisible to attackers since it is a layer 2 bridging device with no IP stack. The honeywall performs *data control* to mitigate the risk of an attacker harming production systems from inside the honeynet.

When any one of the honeypots is targeted by an attacker, it is known immediately since under normal operation the honeypots have no production value or authorised access. All the attacker's activity is recorded to learn attack patterns and new types of attacks. This is known as *data capture*.

*Data analysis* is also performed by the honeynet system to convert any data captured into valuable information to send to the system administrator. Appropriate action is then taken, for example, block the attacker's IP address to prevent any further authorised access to the network.

### V. CONCLUSIONS

IPTV systems on the IMS are targets for attackers. This paper outlined the shortcomings of traditional security techniques and introduced a security framework to adequately secure IPTV systems in the IMS. This solution is based on techniques which have already been developed and proven. The framework uses the honeynet in addition to traditional methods. It fulfills the research goals and secures IPTV systems in the IMS with a layered approach. Further work is required on this topic in order to evaluate the suitability of the framework in a practical implementation.

### REFERENCES

- [1] R. Piconi. "Ultimate Guide to IPTV: A 360-degree view of the IPTV ecosystem". Chapter *IP Multimedia TV: IPTV in an IMS World*, pages 10-14. Horizon House Publications, 2006.
- [2] J. Levine, R. LaBella, H. Owen, D. Contis, B. Culver. "The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks". *Proceedings of the IEEE Workshop on Information Assurance*, 2003.
- [3] N. Veerasamy, J. P. Eloff. "Framework for the Establishment of a Honeynet". *Proceedings of the SATNAC Conference*, 2007.
- [4] C. K. Dimitriadis. "Improving Mobile Core Network Security with Honeynets". *IEEE Security & Privacy*, July/August:40-47, 2007.
- [5] M. Sher, T. Magedanz. "A Vulnerabilities Analysis and Corresponding Middleware Security Extensions for Securing NGN Applications". *Computer Networks*, 51:4697-4709, 2007.
- [6] S. Khattab, R. Melhem, D. Mosse, T. Znati. "Honeypot Back-Propagation for Mitigating Spoofing Distributed Denial-of-Service Attacks". *Journal of Parallel and Distributed Computing*, 66:1152-1164, 2006.
- [7] H. Artail, H. Safa, M. Sraj, I. Kuwatly, Z. Al-Masri. "A Hybrid Honeypot Framework for Improving Intrusion Detection Systems in Protecting Organizational Networks". *Computers & Security*, 25:274-288, 2006.
- [8] Honeynet Project. "Know Your Enemy: Honeynets, what a honeynet is, its value, overview of how it works, and risks/issues involved". [Online]. Available: <http://www.honeynet.org>. [April 2008], 2006.

**Phillippa R. Wilson** obtained her BSc(Elec Eng) degree from the University of Cape Town in 2007. She joined the Communications Research Group at the University of Cape Town as a Telkom Centre of Excellence student where she is currently working towards her MSc(Elec Eng) degree.