

# Correlating Heterogeneous Security Events Using the Prelude IDS Framework

Pierre Chifflier<sup>1</sup> and Sébastien Tricaud<sup>2</sup>

<sup>1</sup> pierre.chifflier@inl.fr

INL

101/103 Bvd MacDonald

75019 Paris, France

<sup>2</sup> sebastien.tricaud@wengo.com

Wengo

40/42 quai du Point du Jour

92100 Boulogne-Billancourt, France

**Abstract.** Today's networks need are fairly big. It varies from home-made programs, to all-in-one integrated solutions. We believe there is no need to replace well working products in your network.

In this paper, we will describe the Prelude IDS architecture, how it can be used to resolve one of the worst issue coming into the computer security area and how every component interact with each other to correlate informations.

**Key words:** IDS, Hybrid IDS, IDMEF, Prelude, Correlation, Management, Assessment

In this sentence we make references to [?], which is from a conference I didn't go to, and also [?].

## 1 Understanding Prelude

Prelude is a full featured Hybrid Intrusion Detection System distributed under the GPL License. It has been designed from the ground up to be optimized for distributed environments, completely modular, robust, and fast.

### 1.1 Definitions

**IDS:** Intrusion Detection System

**HIDS:** Hybrid IDS

**Prelude Framework:**

### 1.2 Overview

Prelude IDS is mainly a library that can be used by any application to directly integrate into what is called the Prelude Framework

**Libraries**

**Manager**

**Sensors**

**Frontends**

### 1.3 Components

**Libprelude** LibPrelude is a library which enables Prelude components to communicate in a standard IDMEF method.

**LibpreludeDB** LibPreludeDB is the database engine for prelude, so that any other Prelude component are data storage and retrieval agnostic.

**Prelude LML** Prelude-LML, or Prelude Log Monitoring Lackey, is a part of the project that deals with the host based intrusion detection aspects. It can listen to the network for Syslog messages coming from different hosts on heterogeneous platforms.

Any system that generates logs from standard Unix/Windows NT Syslog and transmits them to the LML host should be capable of utilizing Prelude-LML analysis engine.

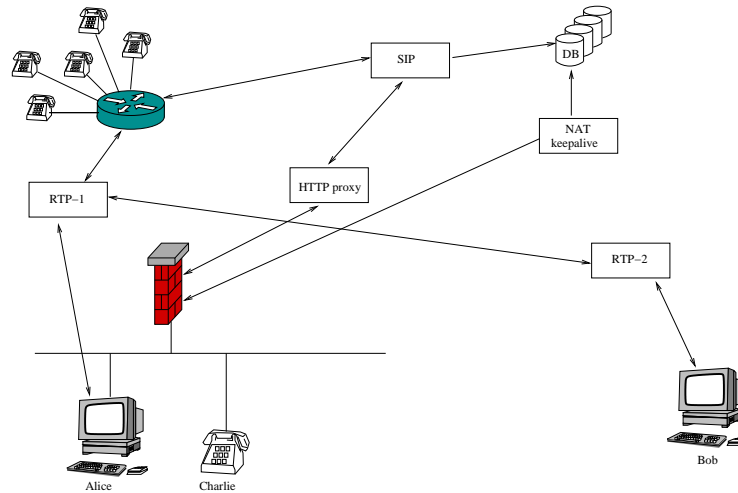
**Prelude Manager** The Manager (there can be several in an IDS network) accepts secured connections from sensors and saves the alerts that Sensors emit. Managers can also forward alerts to CounterMeasure Agents to process and take appropriate actions.

**Prelude Correlator** Prelude Correlator performs the work of reading IDMEF data from Prelude Manager, to trigger an alert from several other.

**Prewikka** Prelude is the Prelude IDS frontend.

## 2 Pragmatic problems current IDS hardly solve

This section covers a practical need for a Prelude IDS deployment in a VoIP environment. First of all, we will quickly describe VoIP requirements. Then, we will see what the problems are and how they can be solved using Prelude IDS.



## 2.1 VoIP Basics

## 2.2 The VoIP Security Challenge

## 2.3 Solving issues

## 3 Events Correlation

Isolation a single alert, such as :

“User login failed with an invalid user (failed)” triggers a MEDIUM alert impact. It not really relevant considering other alerts you have in your network. But, how about a brute force attack occurring ?

## 4 Conclusion

## References