Status report del gruppo di lavoro GARR "sec-sensori"

Alessandro Agostini[1], Federico Bitelli[2], Cecilia Catalano[3], Roberto Cecchini[4], Giacomo Fazio[5], Luigi Gangitano[6], Eleonora Teti[7]

Abstract

Questo report descrive il lavoro svolto dal gruppo di lavoro GARR "sec-sensori". Lo scopo del gruppo è l'istituzione e la gestione (software) di un prototipo di rete di sensori, adatta a costituire un sistema di "*early warning*" per minacce informatiche, quali la diffusione di un nuovo virus o un massiccio attacco DoS

INTRODUZIONE

Questo report descrive il lavoro svolto dal gruppo di lavoro GARR "sec-sensori", nato su proposta di Roberto Cecchini durante il workshop GARR di Roma del Novembre 2003.

Lo scopo del gruppo è l'istituzione e la gestione (software) di un prototipo di rete di sensori, adatta a costituire un sistema di "*early warning*" per minacce informatiche, quali la diffusione di un nuovo virus o un massiccio attacco DoS. In aggiunta, ogni sensore costituirà un sistema di *Network Intrusion Detection* per la sua LAN, dalla gestione il più semplice possibile.

Lo scopo è di sperimentare un servizio che, se ritenuto efficace, potrà poi far parte di quelli offerti dal GARR.

REQUISITI

Le caratteristiche che il sistema deve possedere sono le seguenti:

- semplicità di installazione, manutenzione e aggiornamento;
- affidabilità delle componenti di rilevamento e monitoraggio;
- sicurezza e rispetto della privacy;
- basso impatto economico delle componenti del sistema e dello sforzo necessario alla gestione;
- scalabilità.

Per ridurre gli sforzi di gestione, viene proposta la realizzazione di un centro di distribuzione che provveda a fornire l'installazione e configurazione del Sistema Operativo (su CD-ROM o via rete) e l'aggiornamento automatico del software e delle politiche di monitoraggio.

[1] CNR IFAC, Firenze
[2] Dipartimento di Fisica, Università Roma 3
[3] ISTAT, Roma
[4] INFN, Sezione di Firenze
[5] IASF, Sezione di Palermo
[6] Linux User Group, Università Roma 3
[7] CASPUR, Roma

ARCHITETTURA

L'architettura proposta (Figura 1. Architettura del sistema) è costituita da "sensori" dislocati presso i vari Enti afferenti alla rete GARR e da uno o più punti di raccolta e analisi dati, "collettori", strutturati in diversi livelli di elaborazione (ai livelli più alti vengono forniti dati aggregati).

I sensori distribuiranno i dati con tutti i dettagli richiesti, eventualmente anonimizzati, ai collettori più vicini, che, a loro volta, li invieranno, in forma opportunamente aggregata a quelli di livello superiore.

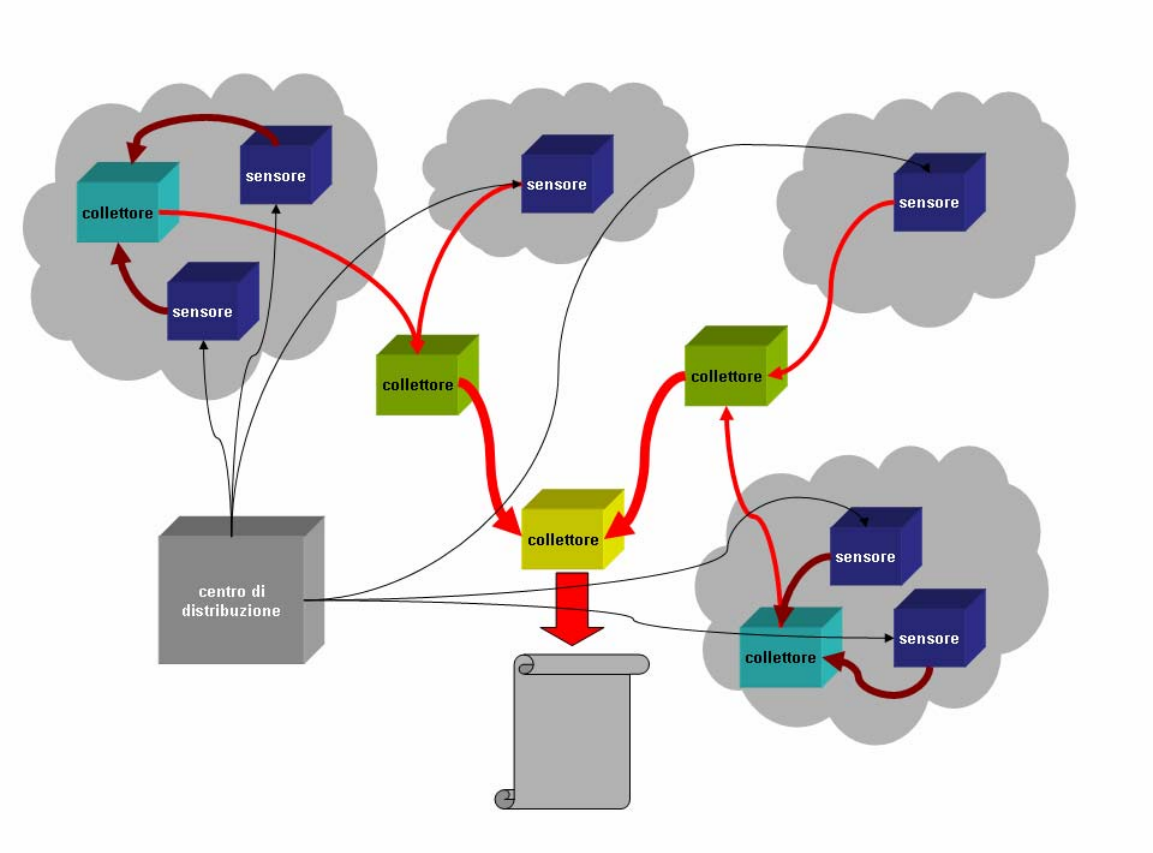

Figura 1. Architettura del sistema

Sensore

La gestione di un sensore dovrà essere la più semplice possibile. Un centro di distribuzione provvederà a fornire il Sistema Operativo (su CD-ROM o via rete) e i file di configurazione del rivelatore vero e proprio. L'aggiornamento sarà automatico.

In conclusione, il sistema dei sensori dovrà essere capace di:

- attuare un meccanismo di download degli aggiornamenti;
- inviare i dati al collettore (eventualmente anonimizzati);
- inviare un report degli allarmi al responsabile locale.

Collettore

Il collettore dovrà essere in grado di:

- disaccoppiare l'output dei sensori dalle elaborazioni successive;
- sintetizzare i dati ricevuti, anonimizzarli e inviarli a quelli di livello superiore;
- generare alert in caso di eventi ritenuti pericolosi.

Il responsabile locale potrà personalizzare la quantità di informazioni ricevute.

Centro di distribuzione

Il centro di distribuzione svolgerà le seguenti funzioni:

- installazione automatica e aggiornamento software dei sensori e collettori;
- aggiornamento delle configurazioni dei sensori.

SCELTE REALIZZATIVE

L'attività del gruppo è consistita nell'individuazione dei prodotti Open Source più adatti per realizzare un prototipo del sistema, scegliendo Linux come piattaforma di riferimento.

Sensori

La scelta è caduta su **snort** [SNO], il più diffuso strumento Open Source per Network Intrusion Detection, per le sue caratteristiche di completezza e semplicità di personalizzazione. Il prodotto è attivamente mantenuto con aggiornamenti molto frequenti delle firme degli attacchi.

Per evitare un numero eccessivo di falsi positivi, si è stabilito di individuare un sottoinsieme significativo di regole ridotto rispetto a quello della distribuzione ufficiale. L'insieme verrà conservato e mantenuto aggiornato presso il centro di distribuzione, al quale il sensore si collegherà periodicamente per aggiornarsi.

Collettori

A livello di collettore sono stati valutati i seguenti prodotti per l'analisi dei log dei sensori:

- **snortsnarf**: un programma in **perl** atto ad elaborare i file contenenti gli alert e di produrre report in HTML;
- **ACID** [ACI] e **BASE** [BAS] : motori di analisi basati su PHP capace di eseguire ricerche e elaborazioni sui dati generati da vari IDS, firewall e network monitoring tool e memorizzati in un database (**MySQL** [MYS], nel nostro caso). Lo sviluppo di **ACID** è fermo e il progetto è stato sostituito da **BASE**.

snortsnarf è risultato troppo primitivo per gli scopi del gruppo e quindi al momento si è scelto di utilizzare la soluzione **ACID**/**BASE** opportunamente arricchita (ad es. con l'anonimizzazione dei dati).

Centro di distribuzione

Per quanto riguarda l'installazione delle macchine si utilizza **FAI** (Fully Automatic Installation) [FAI], un sistema automatizzato di installazione per Debian Gnu/Linux.

I passi per l'installazione sono i seguenti:

- su un modulo web l'amministratore locale indica i parametri di rete del sensore;
- il server **FAI**, partendo da queste informazioni, provvede a creare una immagine di floppy di boot che è inviata all'indirizzo e-mail indicato nel modulo;
- il client, all'avvio dal floppy, monta via NFS il root filesystem dal server **FAI** (è quindi necessario che sia in grado di usare NFS con server al di fuori della propria LAN);
- successivamente gli script di **FAI** si occupano dell'installazione senza che sia necessaria nessuna ulteriore operazione manuale: in particolare, vengono partizionati gli hard disk,

viene installato il sistema base e i pacchetti aggiuntivi. Il client così installato usa come mirror Debian per il download dei pacchetti il server **FAI** stesso;
- il server **FAI** personalizza la configurazione del client.

Per quanto riguarda l'aggiornamento del software il centro di distribuzione svolge la funzione di mirror Debian per i pacchetti utilizzati e personalizzati. I sensori sono configurati in modo da collegarvisi periodicamente.

Le regole di **snort** sono aggiornate sul centro di distribuzione utilizzando **oinkmaster** [OIN], che permette di conservare le personalizzazioni preesistenti, e distribuite ai client, sotto forma di pacchetto Debian, con le modalità di un aggiornamento software.

Trasferimento dati

I sensori e i collettori comunicano tramite **SAFT/sendfile** [SFI], un tool per la trasmissione asincrona di file. In questo caso è preferibile a **rsync**, perché elimina le complicazioni del meccanismo di autenticazione (ad es. lo scambio di chiavi), pur mantenendo un idoneo livello di sicurezza.

CONCLUSIONI

A seguito delle scelte sopra indicate, attualmente è stato realizzato il centro di distribuzione, che utilizza **FAI** per l'installazione dei sensori, mentre, per quanto riguarda i collettori, è stato modificata la distribuzione di **ACID** per ottimizzare e anonimizzare i dati raccolti.

Rimane da mettere a punto un sistema di installazione alternativo a nfs e restano da risolvere i problemi di scalabilità (uso di una gerarchia di collettori).

Riteniamo che una rete geograficamente diffusa di sensori possa avere importanti impieghi per la segnalazione tempestiva di anomalie potenzialmente dolose, con ricadute positive sulle singole realtà locali, senza richiedere competenze specifiche o aggravi del carico di lavoro.

BIBLIOGRAFIA

[ACI]
http://acidlab.sourceforge.net/
[BAS]
http://secureideas.sourceforge.net/
[FAI]
http://www.informatik.uni-koeln.de/fai/
[MYS]
http://dev.mysql.com/
[OIN]
http://oinkmaster.sourceforge.net
[SFI]
http://www.belwue.de/projekte/saft/index-us.html
[SNO]
http://www.snort.org

BIOGRAFIE DEGLI AUTORI

Alessandro Agostini

Informatico, System and Network Administrator presso l'IFAC CNR di Firenze. Dal 1984 presso l'IFAC dal 1991 responsabile per la Posta Elettronica dell'istituto. Responsabile dei Servizi di rete.

Dal 2003 collaboratore per la gestione della rete dell'Area di ricerca del CNR di Firenze di cui e' anche APM-GARR.

Federico Bitelli

Fisico, System and Network Administrator presso il Dipartimento di Fisica dell'Università Roma Tre. Dal 2002 responsabile tecnico dei Servizi Informatici. In precedenza collaboratore con il Centro di Calcolo INFN Sezione Roma 3.

Cecilia Catalano

Laureata in Ingegneria Elettronica, lavora presso l'ISTAT dal 2001 nel Servizio Gestione e Standardizzazione dei Sistemi Informatici.

Roberto Cecchini

Laureato in Fisica, è responsabile del Servizio Calcolo e Reti della Sezione INFN di Firenze, dal 1999 è responsabile del servizio di sicurezza informatica della rete GARR (GARR-CERT), dal 1998 gestisce la Certification Authority dell'INFN (INFN CA).

Giacomo Fazio

Informatico, System and Network Administrator presso lo IASF, sezione di Palermo. Responsabile per la Posta Elettronica dell'intero IASF CNR. Responsabile dei Servizi di Calcolo IASF Palermo. Dal 1991 presso l'IFCAI, poi divenuto IASF ora INAF. In precedenza programmatore per i gruppi di Ricerca operanti nel campo dell'Astrofisica.

Luigi Gangitano

Membro del nucleo del Lug Roma 3, consulente presso Open Consulting S.r.l., esperto di networking e sicurezza.

Eleonora Teti

Ha conseguito la Laurea in Ingegneria Informatica discutendo una tesi, svolta in collaborazione con CASPUR, sull'implementazione distribuita di un sistema di sicurezza. Dal 2003 collabora con il CASPUR e si occupa di Network Intrusion Detection System e Network Monitoring