Gruppo *sec-sensori*: status report

Roberto Cecchini

GARR_05

Pisa, 12 Maggio 2005

I membri attivi

- Alessandro Agostini (CNR IFAC, Firenze)
- Federico Bitelli (Dip.to di Fisica, Roma3)
- Guido Buscema (INAF, Roma)
- Cecilia Catalano (ISTAT, Roma)
- Roberto Cecchini (INFN, Firenze)
- Giacomo Fazio (IASF, Palermo)
- Luigi Gangitano (LUG, Roma 3)

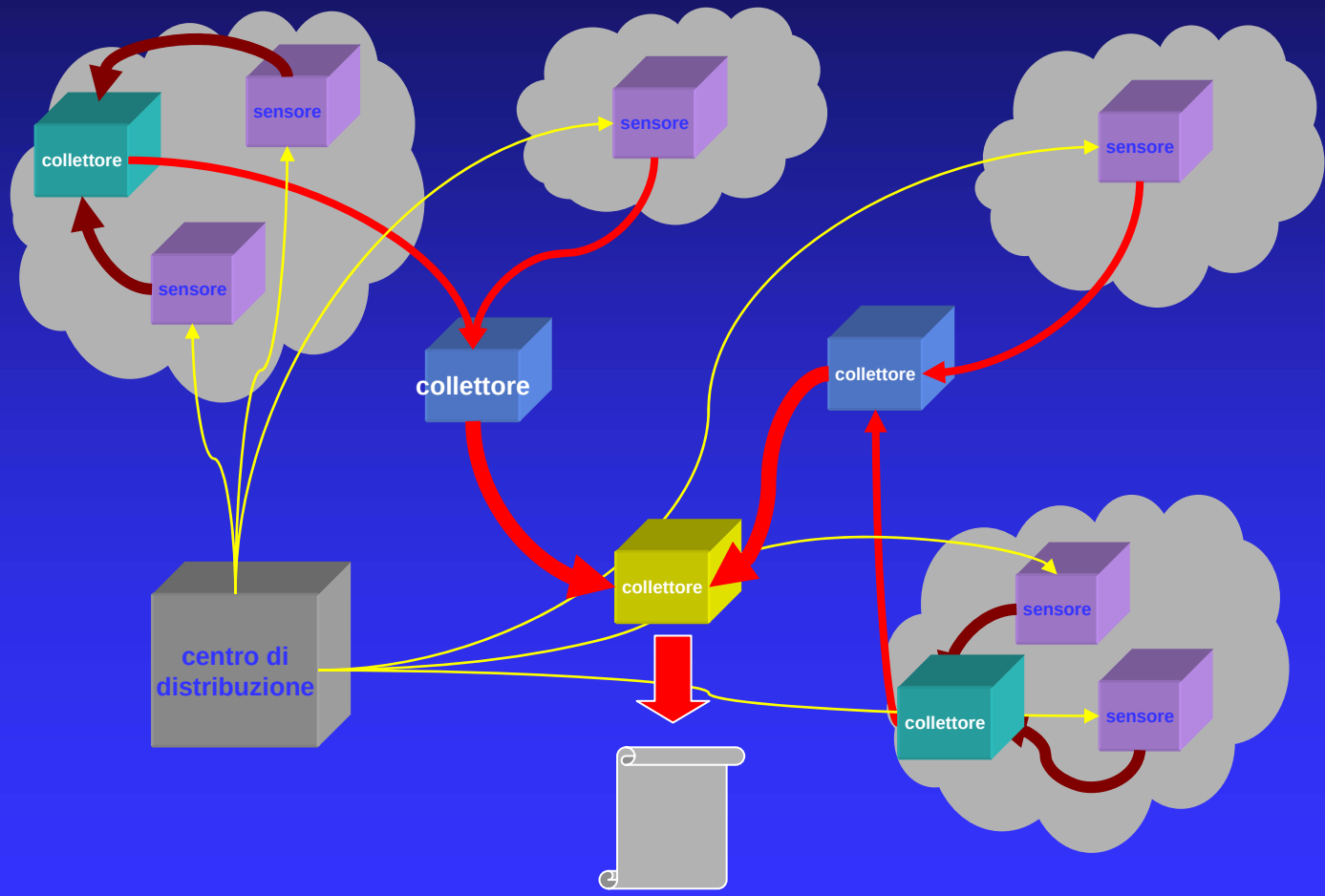
Scopo

- Istituzione e gestione di un prototipo di rete di “sensori”
  - “*early warning*” per minacce informatiche;
  - sistema di *Network Intrusion Detection* per la propria LAN.
- Sperimentare un servizio che, se ritenuto efficace, potrà far parte di quelli offerti dal GARR.

Requisiti

- 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.

Architettura 1/2



Architettura 2/2

- **Centro di distribuzione**
  - installa e aggiorna il software dei sensori e collettori;
  - aggiorna le configurazioni dei sensori.
- **Sensore**
  - scarica automaticamente gli aggiornamenti;
  - invia i dati al collettore (eventualmente anonimizzati);
  - invia un report degli allarmi al responsabile locale.
- **Collettore**
  - disaccoppia l'output dei sensori dalle elaborazioni successive;
  - sintetizza i dati ricevuti, li anonimizza e li invia a quelli di livello superiore;
  - genera alert in caso di eventi ritenuti pericolosi.

Scelte: sensori e collettori

- Sensori
  - **snort**
    - sottoinsieme di regole rispetto a quello della distribuzione ufficiale.
- Collettori
  - **snortsnarf**
  - **ACID** e **BASE**
    - opportunamente arricchiti (ad es. con l'anonimizzazione dei dati).

Scelte: centro di distribuzione

- Installazione software: **FAI** (Fully Automatic Installation)
  - un sistema automatizzato di installazione per Debian Gnu/Linux.
- Mirror per i pacchetti utilizzati e personalizzati: i sensori sono configurati in modo da collegarvisi periodicamente.
- Le regole di **snort** aggiornate via **oinkmaster.**
- Trasferimento dati: **SAFT/sendfile**
  - invia file in modo asincrono
  - ogni sensore invia periodicamente i log in un'apposita directory sul collettore di riferimento
  - più semplice di **rsync.**

Stato dei lavori

- Fatto:
  - centro di distribuzione;
  - modificato **ACID** per ottimizzare e anonimizzare i dati raccolti;
  - rete geografica sperimentale di nodi.
- Da fare:
  - sistema di installazione alternativo a **nfs;**
  - risolvere i problemi di scalabilità;
  - sistema di analisi e correlazione dei dati.

Conclusioni

- 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.
- **Abbiamo bisogno di volontari!**