Politiche di sicurezza sugli apparati di rete: l'esperienza dell'area della ricerca di Pisa

Incontro di lavoro sulla sicurezza informatica

13 novembre 2003

CNR-Area della ricerca di Pisa

marco.sommani@iit.cnr.it +39 050 3152127

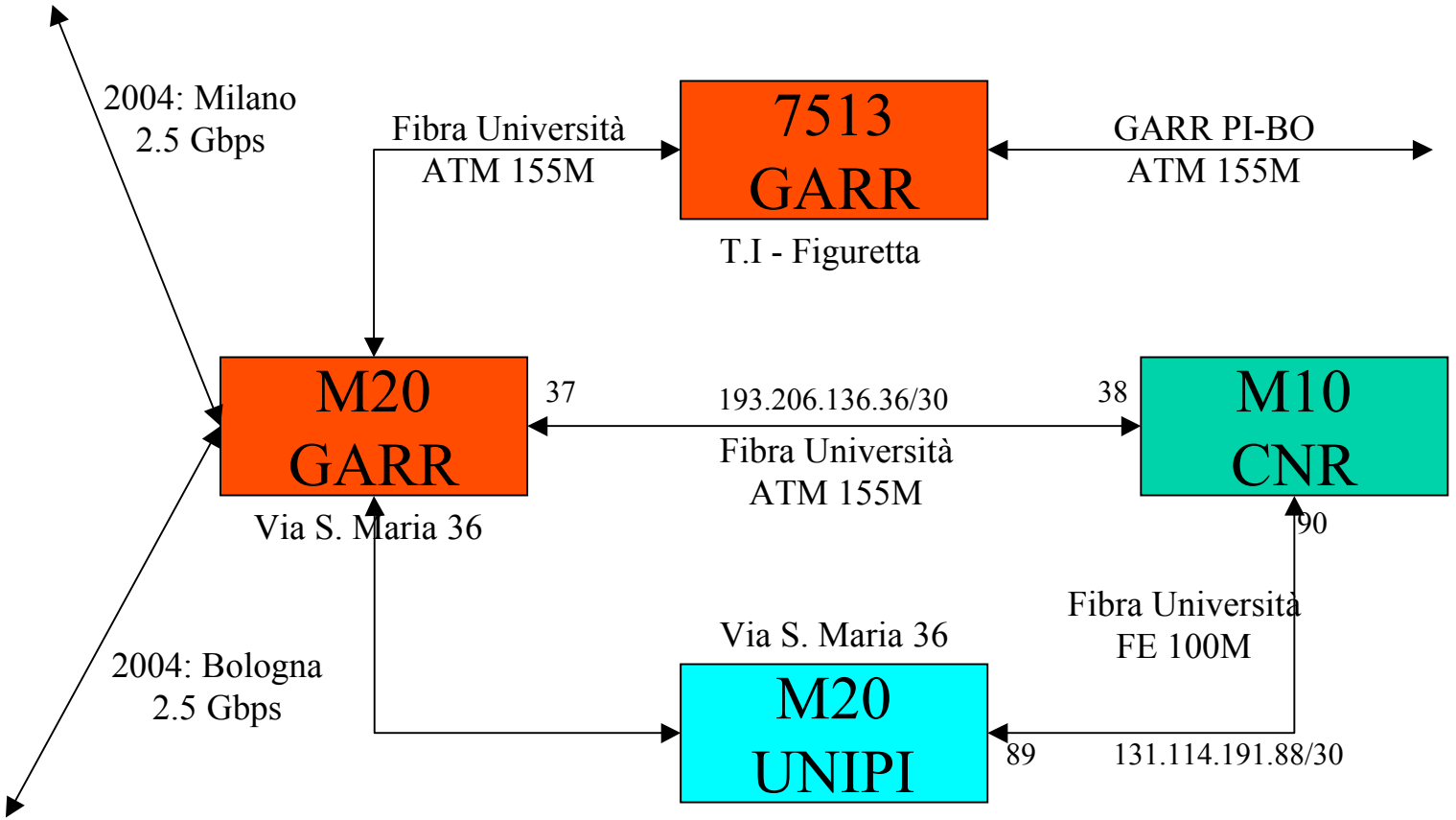
Peculiarità delle aree di ricerca

- Non esiste una politica di sicurezza valida per tutti i ricercatori di un'area.
- La Acceptable Use Policy (AUP) del GARR non contiene norme riguardanti la sicurezza:
  - http://www.garr.it/docs/garr-aup-00.shtml
- Ogni ricercatore collabora con altri gruppi esterni all'area utilizzando la rete nei modi più vari.
- Spesso un ricercatore è in competizione con i colleghi del suo stesso istituto.

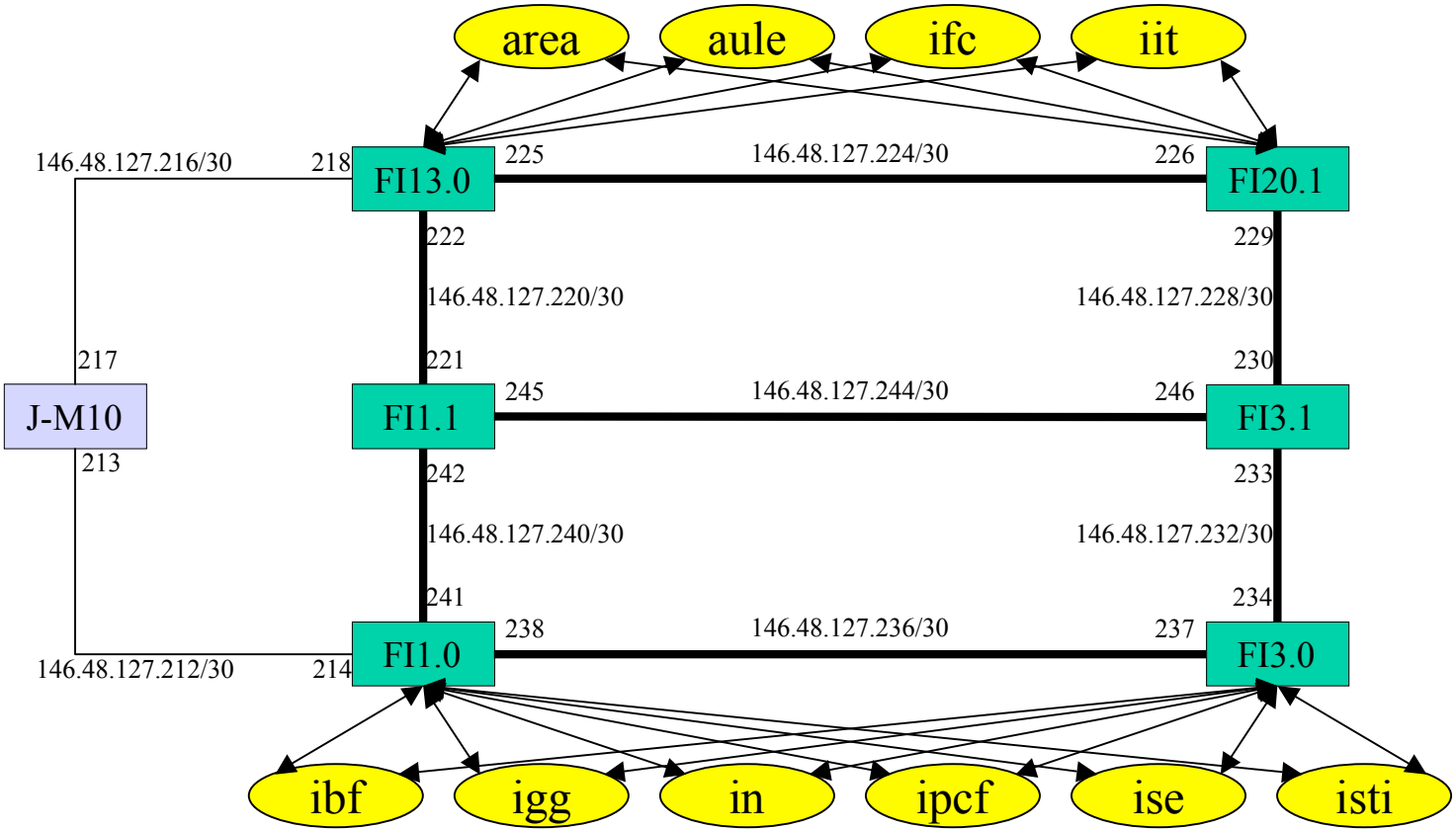
Collegamenti verso l'esterno

- I collegamenti esterni dell'Area (GARR e Università di Pisa) arrivano al CED e sono attestati su un router Juniper M10
- Due link GE collegano il Juniper al FastIron dell'armadio T13.0 (CED) e a quello dell'armadio T1.0 (zona IPCF)

Collegamenti esterni



Schema rete interna



Uso dei router come firewall

- I router Juniper e Foundry Networks dell'Area possono essere usati come firewall "stateless"
  - fw stateless: decide senza ricordare cosa è transitato
  - fw stateful: ricorda cosa è transitato e analizza il campo dati dei protocolli che negoziano gli indirizzi IP e/o i port number (FTP, H.323 etc)
- Una scheda da $ 35.000,00 potrebbe trasformare il Juniper in firewall stateful
- Attualmente le decisioni sono prese analizzando le informazioni di livello 3 e 4

Scuole di pensiero sul filtraggio

- scuola restrittiva: consentire solo quei flussi noti come effettivamente necessari
- scuola liberista: vietare solo quei flussi noti come effettivamente dannosi
- l'esperienza dell'Area porta a una filosofia di compromesso, tendente a dare la preferenza alla scuola liberista

Attuali politiche di filtraggio

- controllare gli indirizzi sorgente
- bloccare i “port number” notoriamente usati per la propagazione dei worms
- su richiesta dei responsabili delle reti degli istituti, proteggere gli utenti ingenui che possono avere attivato inconsapevolmente server ftp, telnet, web, smtp, netbios, etc...
- bloccare i tentativi di apertura di connessioni tcp dall’esterno verso porte elevate di macchine interne
- limitare il traffico dei flussi “poco istituzionali” (scambi di musica, video etc.)

Cosa abbiamo imparato

- La protezione è tanto più efficace quanto più è vicina al dato da proteggere
- È importante avere la massima cura nella configurazione delle macchine di utente
- La cultura di base necessaria per la protezione delle macchine dovrebbe essere diffusa anche fra chi ha scarse conoscenze informatiche
- Il fatto di sapere che i router effettuano filtraggi induce molti utenti a trascurare la protezione delle loro macchine

Monitoraggio

- Per scoprire la presenza di traffici anomali o potenzialmente pericolosi si possono sfruttare le funzioni di monitoraggio disponibili su alcuni router
- Le tecniche attualmente in uso per monitorare il traffico dei router dell'Area sono:
  - MRTG (http://www.mrtg.org/)
  - NTOP (http://(www.ntop.org/)
  - SFLOW (rfc3176, http://www.sflow.org/)

Acquistare un firewall?

- Prima dell'acquisto occorre avere le idee chiare su cosa si vuole proteggere e in che modo
- Tenere presente che un firewall con NAT rende impossibili vari usi leciti della rete
- Il throughput deve essere tale da non costituire un collo di bottiglia
- Mantenere aggiornato il software del firewall
- Se la rete protetta ha indirizzi pubblici, scegliere un firewall con i protocolli di routing OSPF (per l'unicast) e PIM-SM (per il multicast)
- Monitorare l'attività del firewall