Sperimentazione ed estensione del modello IENA per la sicurezza di una rete locale

Relatore:
Prof. Walter Cerroni

Presentato da:
Ivano Manca

Obiettivi della sicurezza informatica

- proteggere i servizi informativi e risorse di rete;
- garantire: autenticità, confidenzialità, integrità;

Obiettivi dell'elaborato

- Estensione di IENA: software per la sicurezza informatica (made in Ce.Se.NA);
- garantire: autenticità, confidenzialità, integrità all'interno del sistema IENA...

Chi attacca e come

- Chi: Hackers, Crackers, Lamers
- Come:
  - ✶“service exploitation”
  - ✶“denial of services”
  - ✶“malware” (virus, worm, trojan)

DIFESA: Politiche tradizionali vs IENA

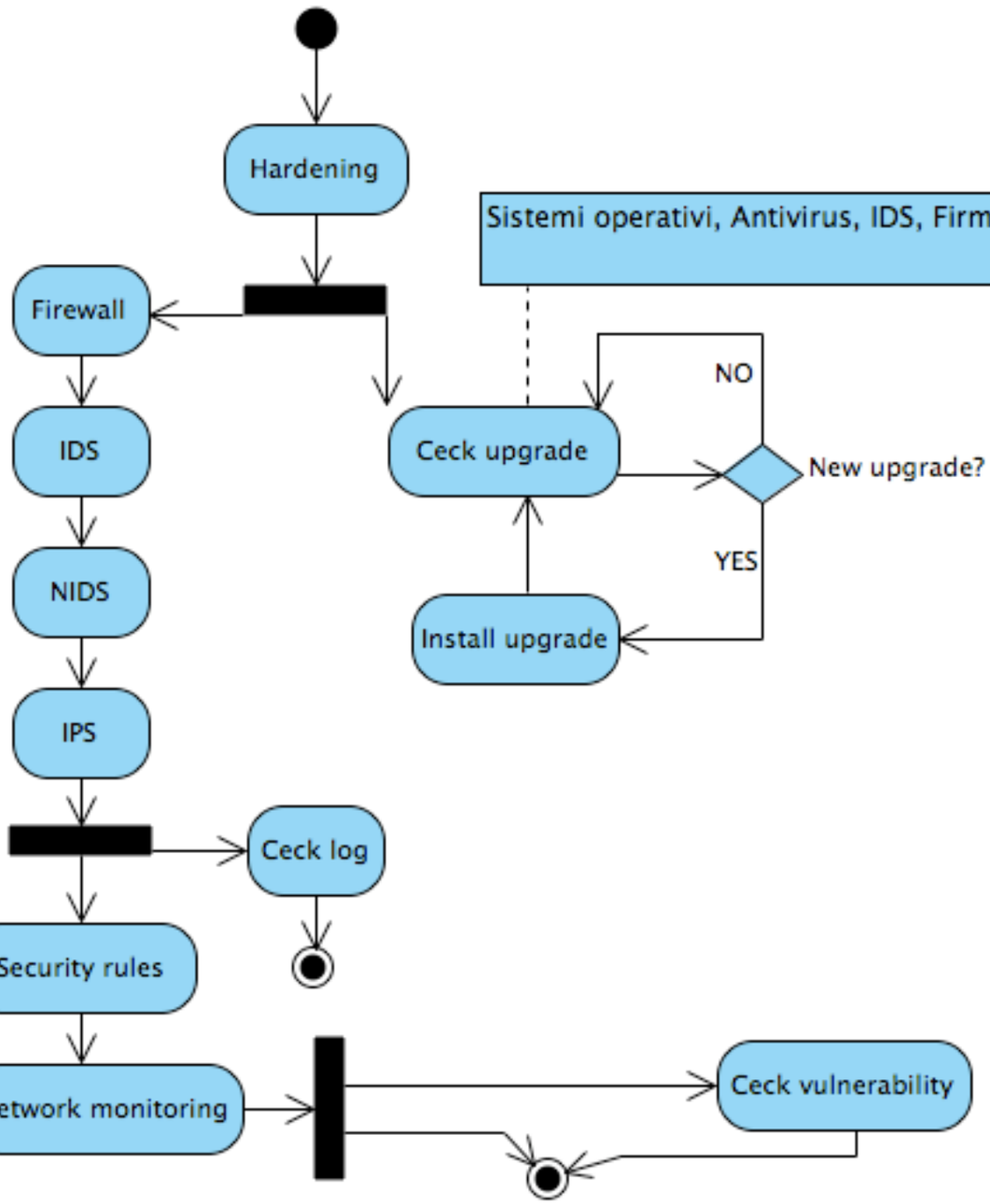
Politiche "chiuse" (sistemi "blindati"):

- Controllo degli accessi;
- Chiusura servizi;
- molteplicità di passwords.

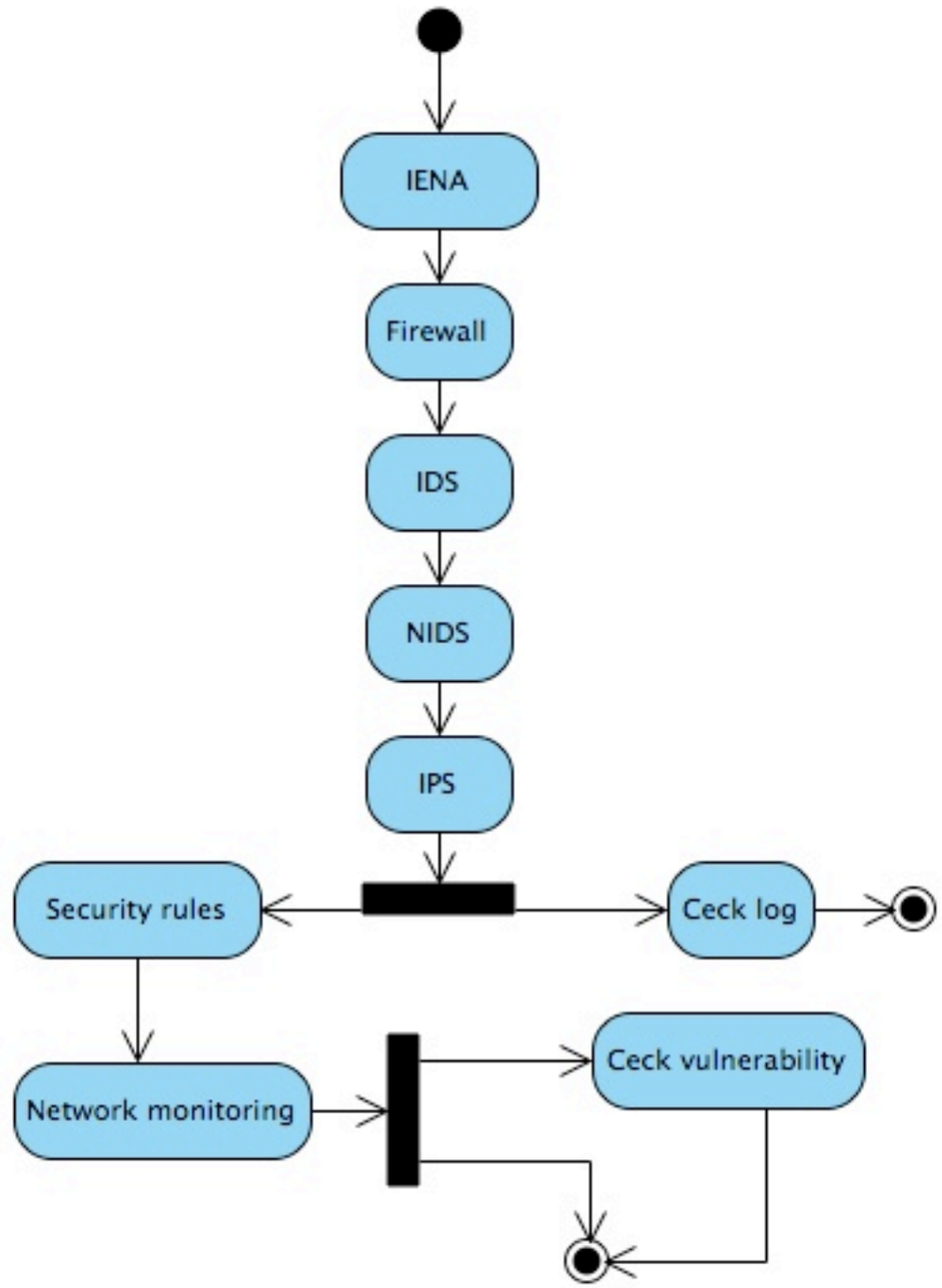
Politica di totale "apertura" (inganno):

- "*prevenire è meglio che curare!*";
- i servizi come strumento di difesa

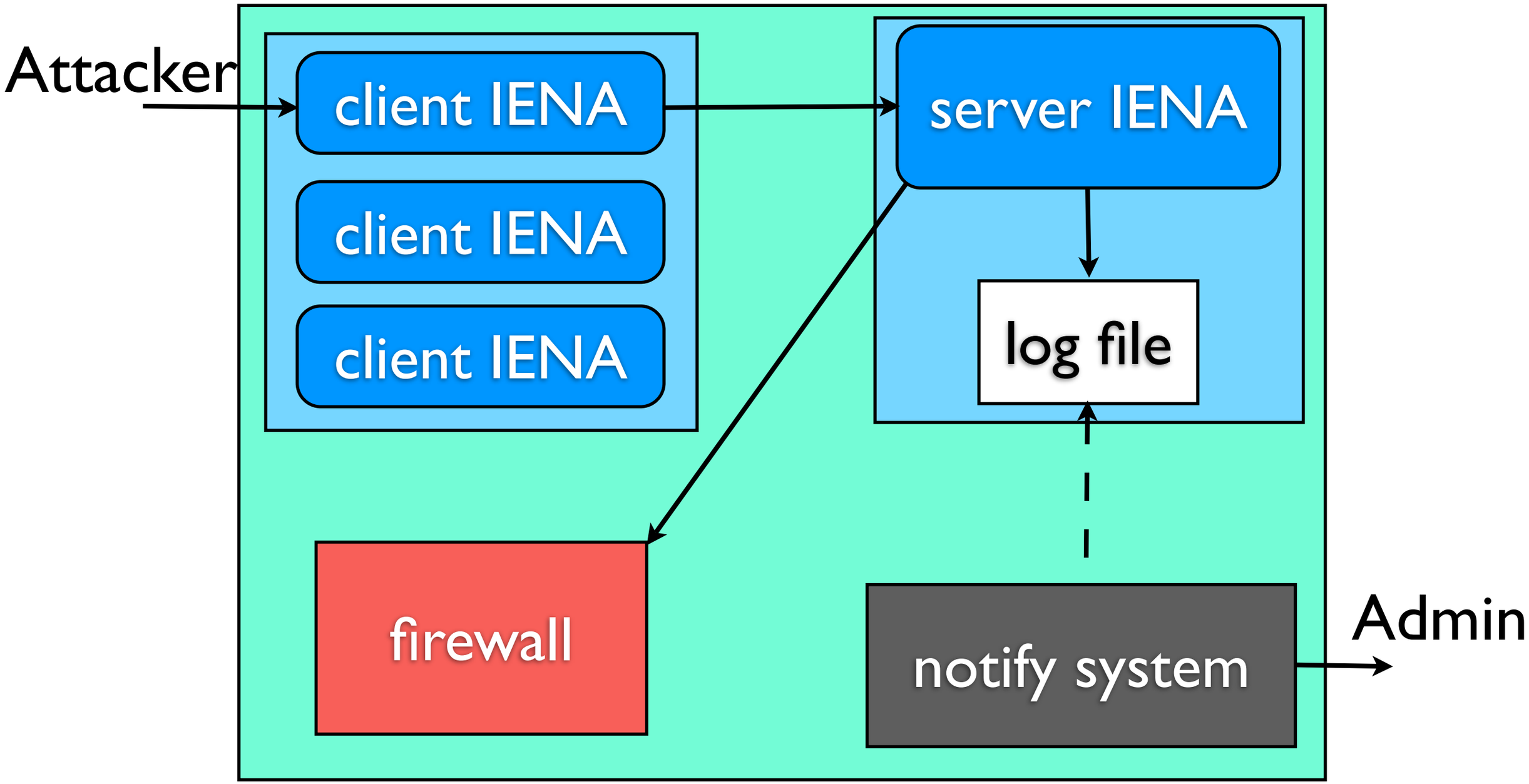
Modello tradizionale per la sicurezza



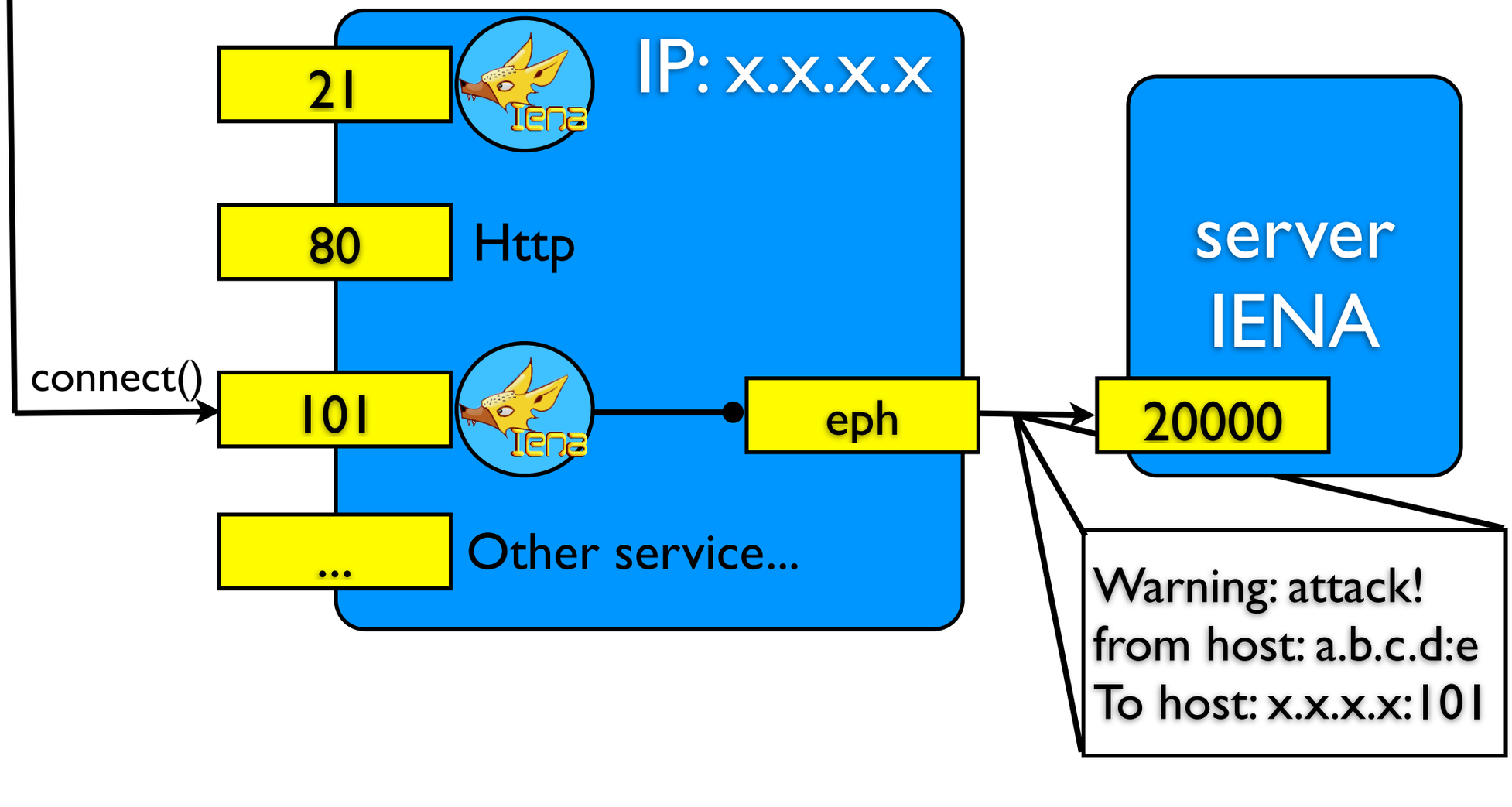
Modello innovativo



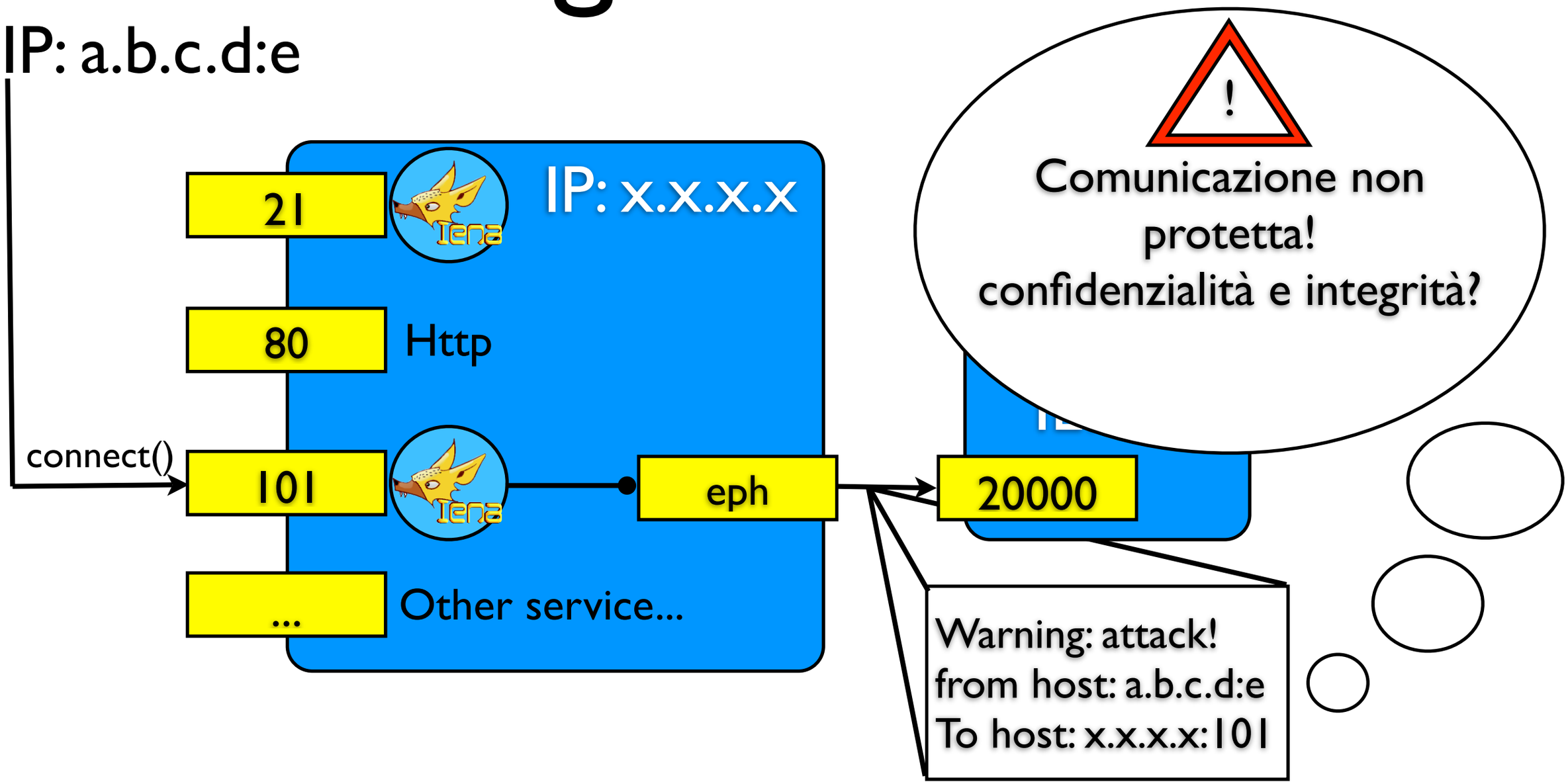
IENA: comportamento



Come vengono rilevati gli attacchi?



Come vengono rilevati gli attacchi?



Estensione del progetto

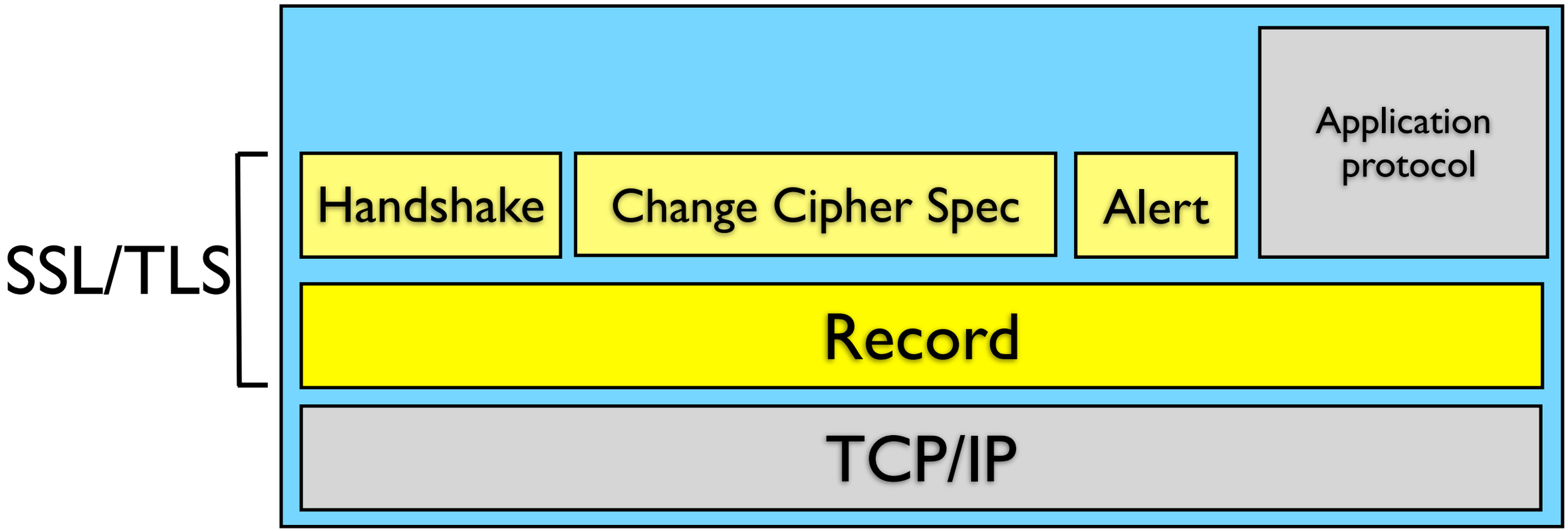
PRIMA IMPLEMENTAZIONE

- serverIENA (C) + log su file;
- clientIENA (Java);
- Comunicazione client/ server in chiaro: utilizzo di semplici Socket ().

PRIMA ESTENSIONE

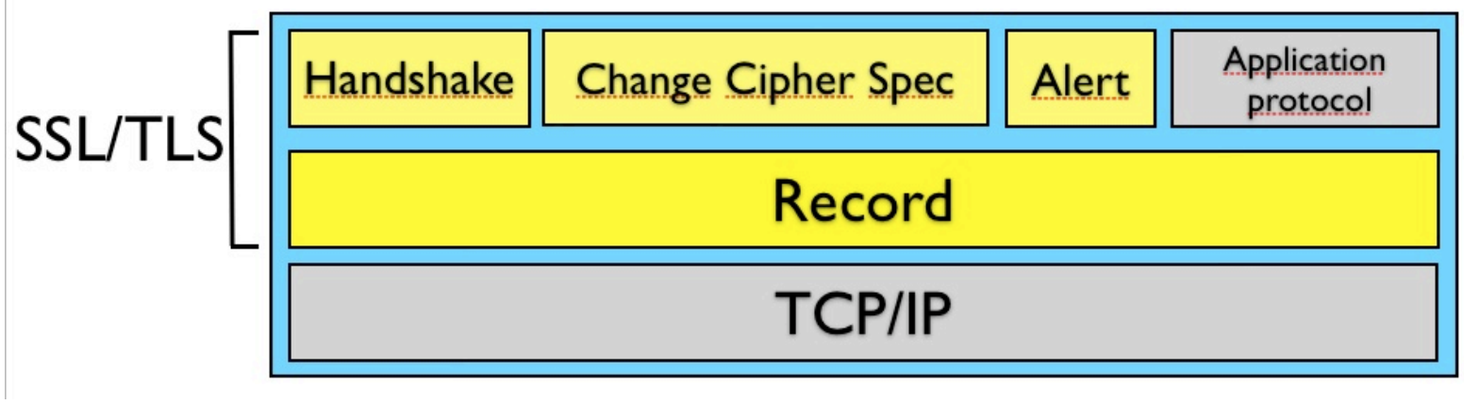
- ★serverIENA (Java) + log su file;
- clientIENA (Java);
- ★Comunicazione client/ server protetta: SSL/TLS (mutual authentication)

Secure Socket Layer (SSL)



SSL: sub-protocols

- RECORD: frammenta, comprime, aggiunge MAC (private key), cifra (simmetric key), aggiunge header.
- ALERT: notifica gli errori: warning/fatal.
- CHANGE CIPHER SPEC: aggiorna le suites per la cifratura;



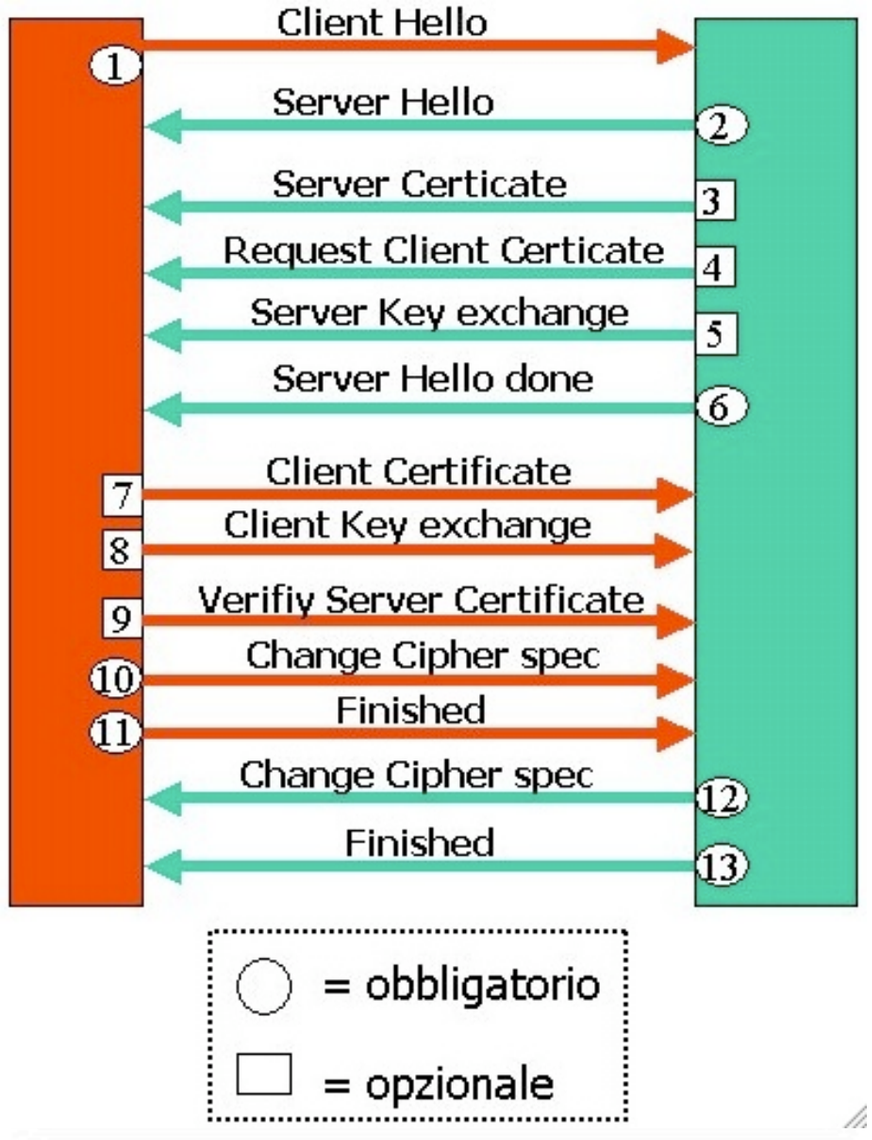
SSL: Handshake

- Fase I[1-2]:
  SLLvx.x, cipher suites, compression method;

- Fase II[3-6]: server authentication, key exchange (simm.);

- Fase III[7-9]: client authentication, key exchange;

- Fase IV[10-13]: cipher spec, chiusura handshake (csprot.).



Scelta delle tecnologie

Perchè Java?

- Indipendenza piattaforma (JVM);
- linguaggio "*open source*" (...finalmente!);
- networking libraries;

Java Secure Socket Extension

- Implementa SSL/TLS;
- Opera a livello di rete;

Java Keytool - KCMT

- Gestione di chiavi e certificati.

Simulazione attacco

★L'attaccante effettua un "port scan"

★I servizi ftp, ndmp, entextxid, italk sono delle trappole! (client IENA).

★L'attaccante crede di aver trovato le vulnerabilità, invece...

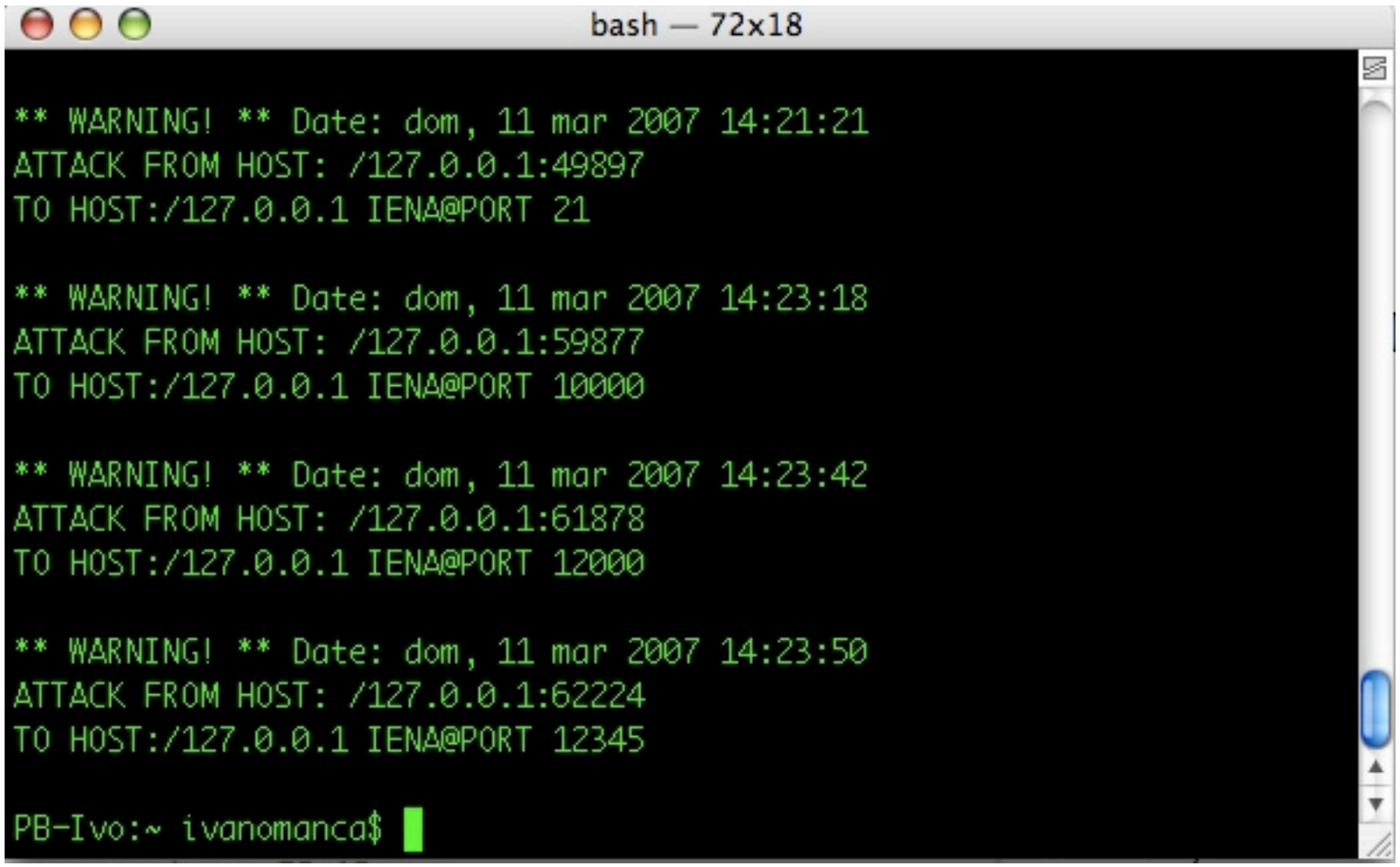
```
Esamina Porte avviato ...

Port Scanning host: 127.0.0.1

     Open TCP Port:     21        ftp
     Open TCP Port:     22        ssh
     Open TCP Port:     548       afpovertcp
     Open TCP Port:     631       ipp
     Open TCP Port:     1033          netinfo-local
     Open TCP Port:     10000         ndmp
     Open TCP Port:     12000         entextxid
     Open TCP Port:     12345         italk
Esamina Porte completato ...
```

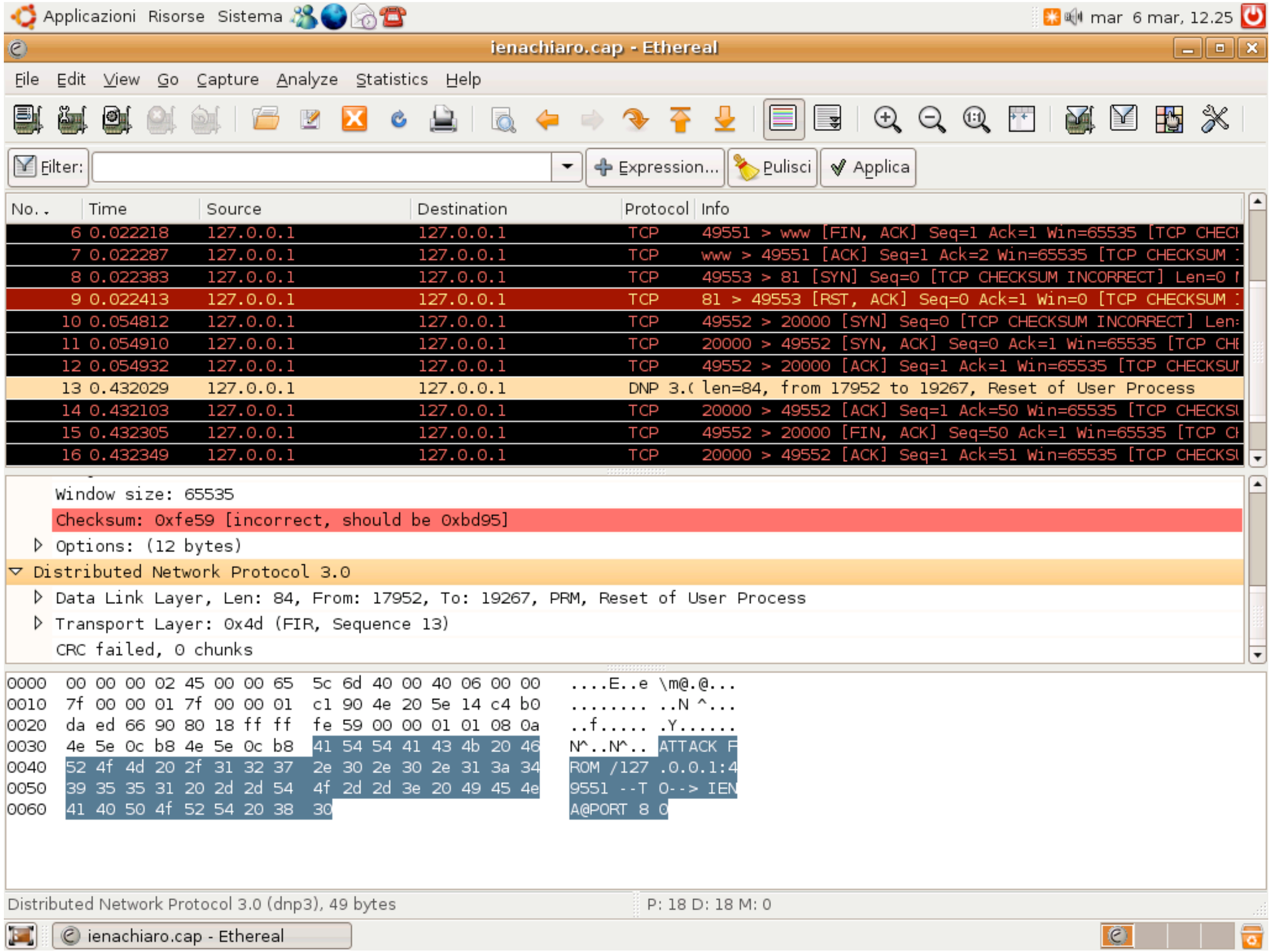
Risposta di IENA

... l'attaccante è stato già espulso da IENA!

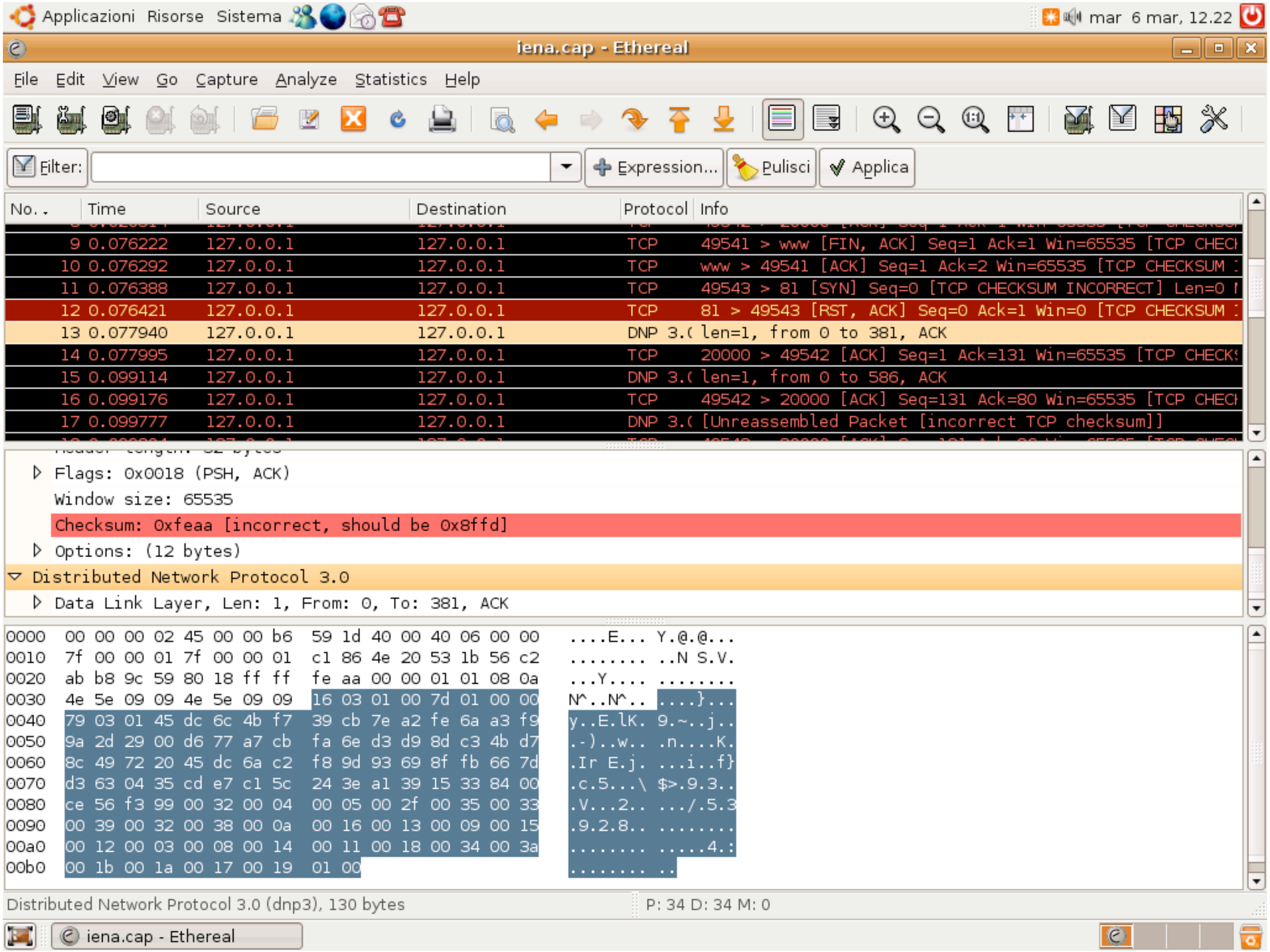


Il server IENA logga l'attacco e modifica immediatamente le regole del firewall. In poco tempo l'amministratore è informato dal sistema di notifica.

Implementazione precedente: connessione in chiaro

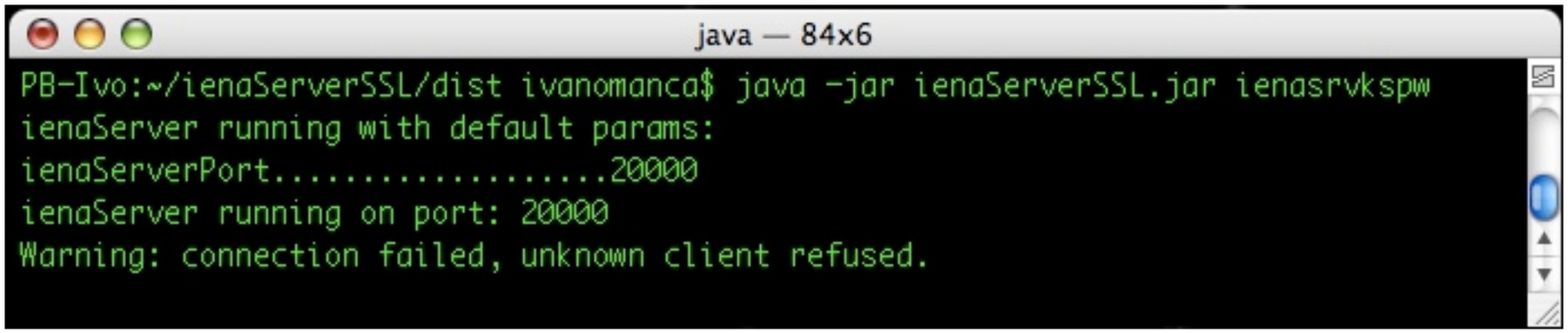


Estensione: connessione sicura (SSL/TLS)



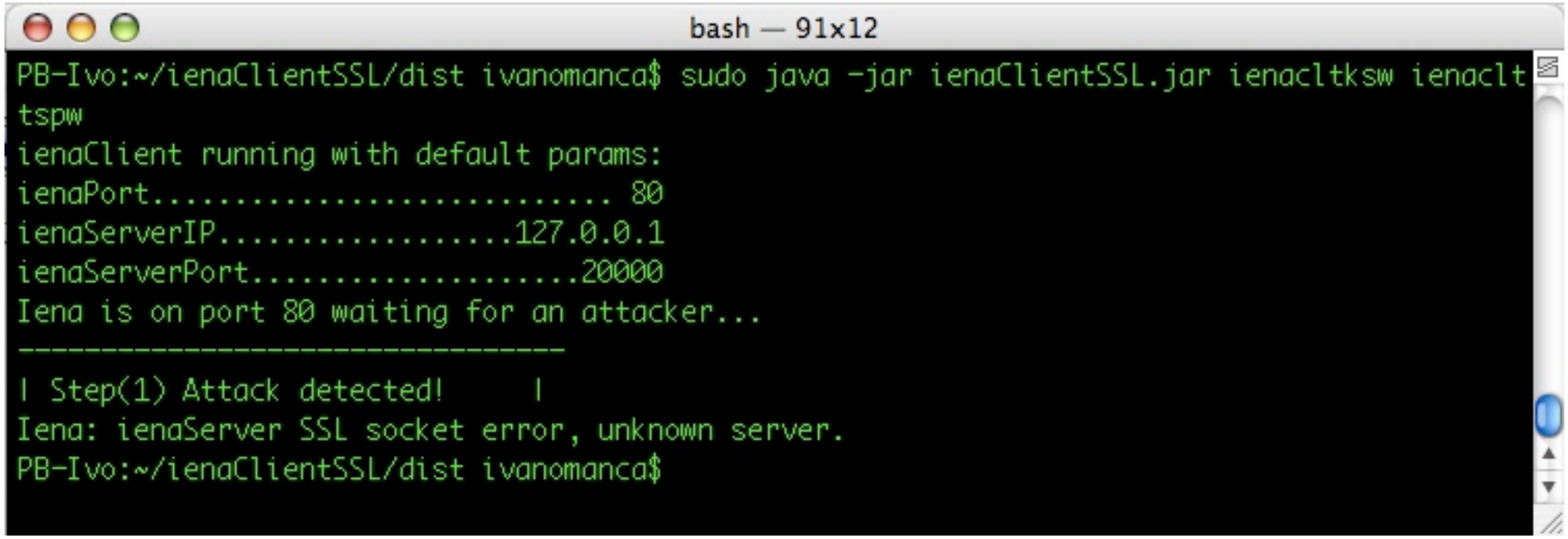
Autenticazione clientIENA/serverIENA

- Un client qualsiasi tenta una connessione al serverIENA...



...serverIENA rifiuta la connessione perchè si tratta di un client unknown.

- Il clientIENA tenta una connessione al suo serverIENA...



...per clientIENA la connessione termina istantaneamente: server unknown.

Sviluppi futuri

Estensioni:

- firewalls plugin;
- notify system plugins;
- installation GUI;
- IENA/Knock integration;
- IENA/IDS/IPS integration.

IENA open source project:

- Website project: http://iena.sourceforge.net

Conclusioni

Modello IENA:

- politica “aperta”;
- semplicità concettuale;
- leggerezza del software.

Estensione di IENA:

- più sicurezza (SSL/TLS);
- maggiore portabilità (JVM);
- maggiore visibilità (“Open source”).