

# 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

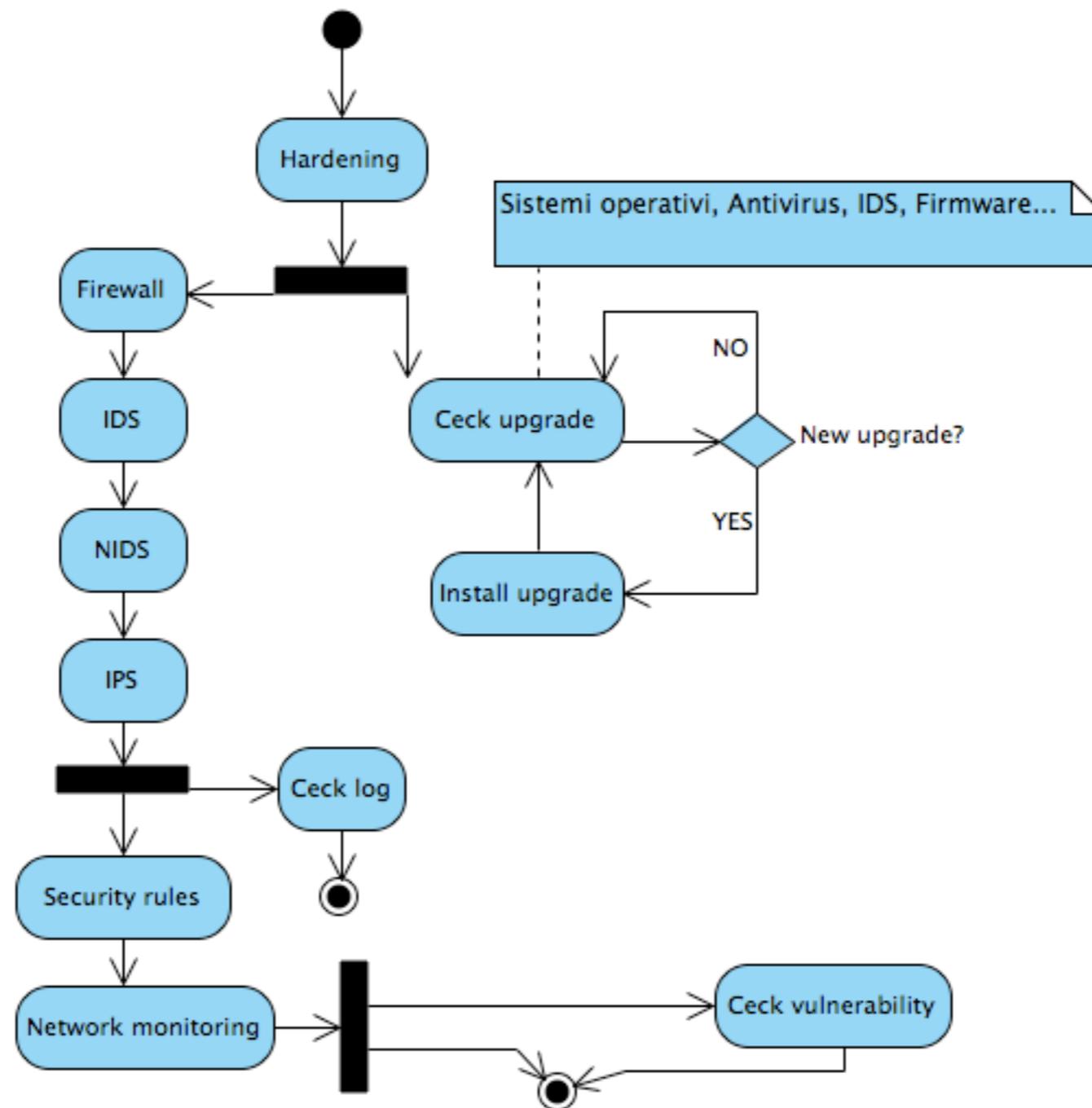
Politiche “chiuse” (sistemi “blindati”):

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

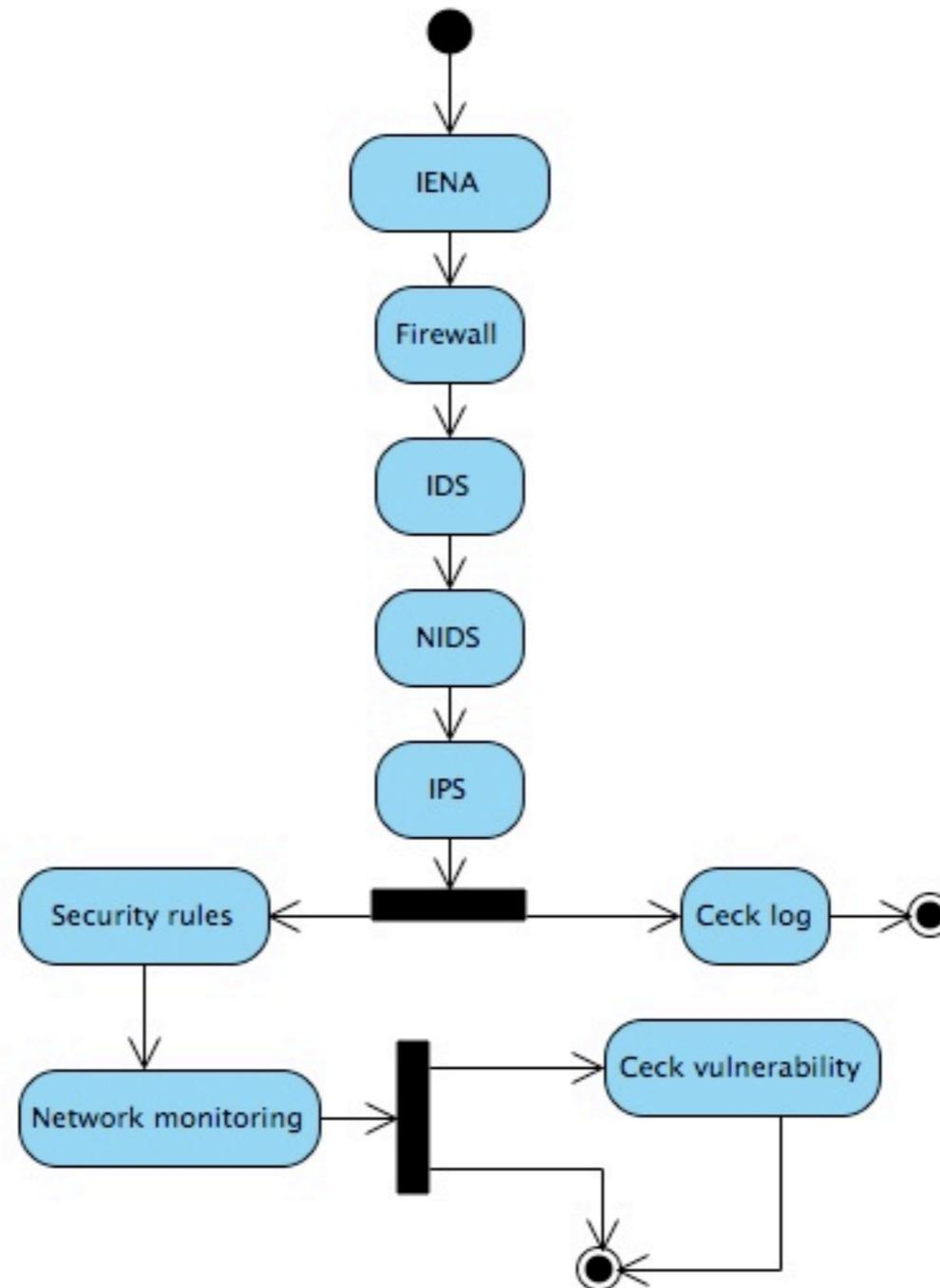
Politica di totale “apertura” (inganno):

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

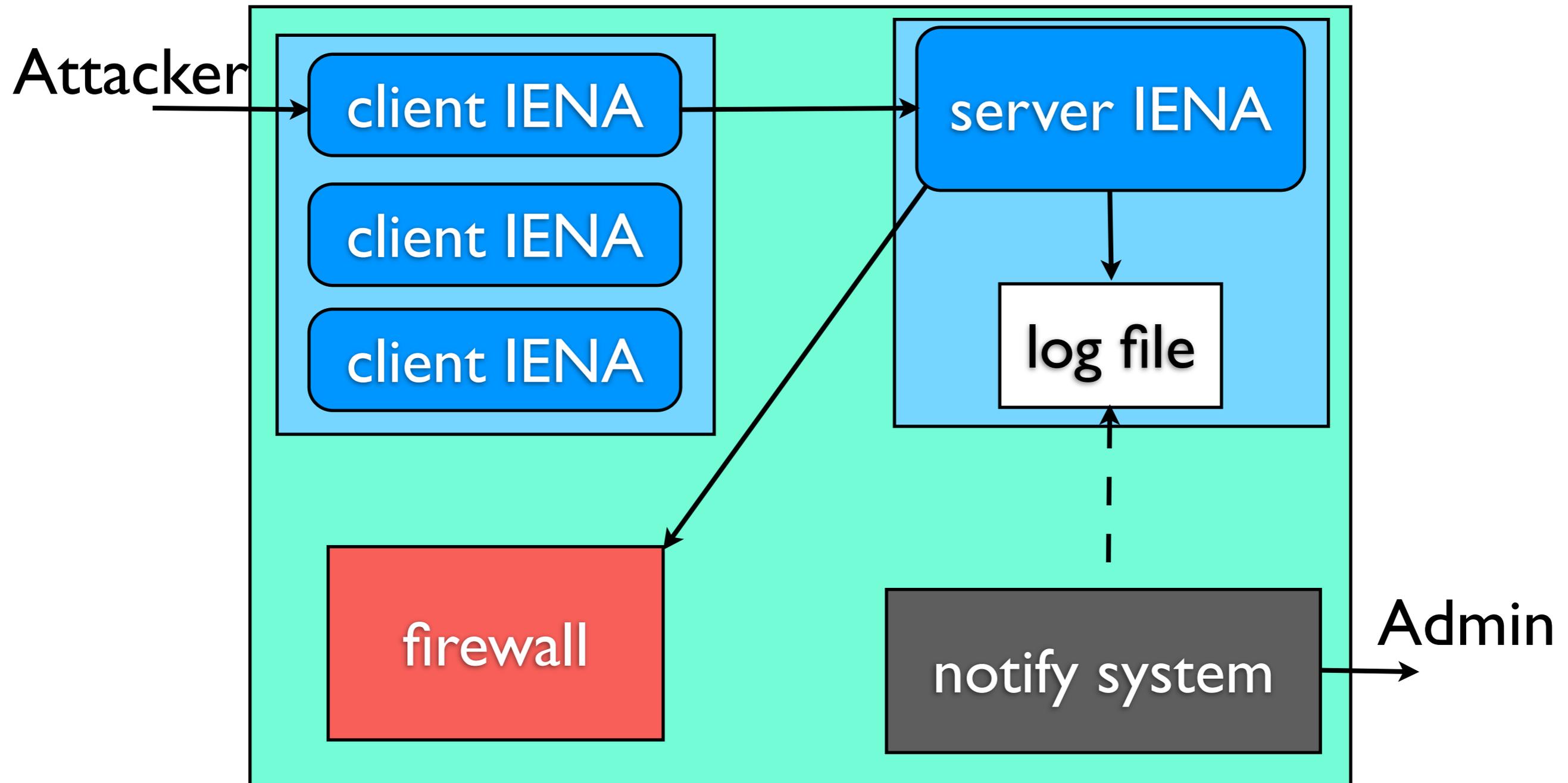
# Modello tradizionale per la sicurezza



# Modello innovativo

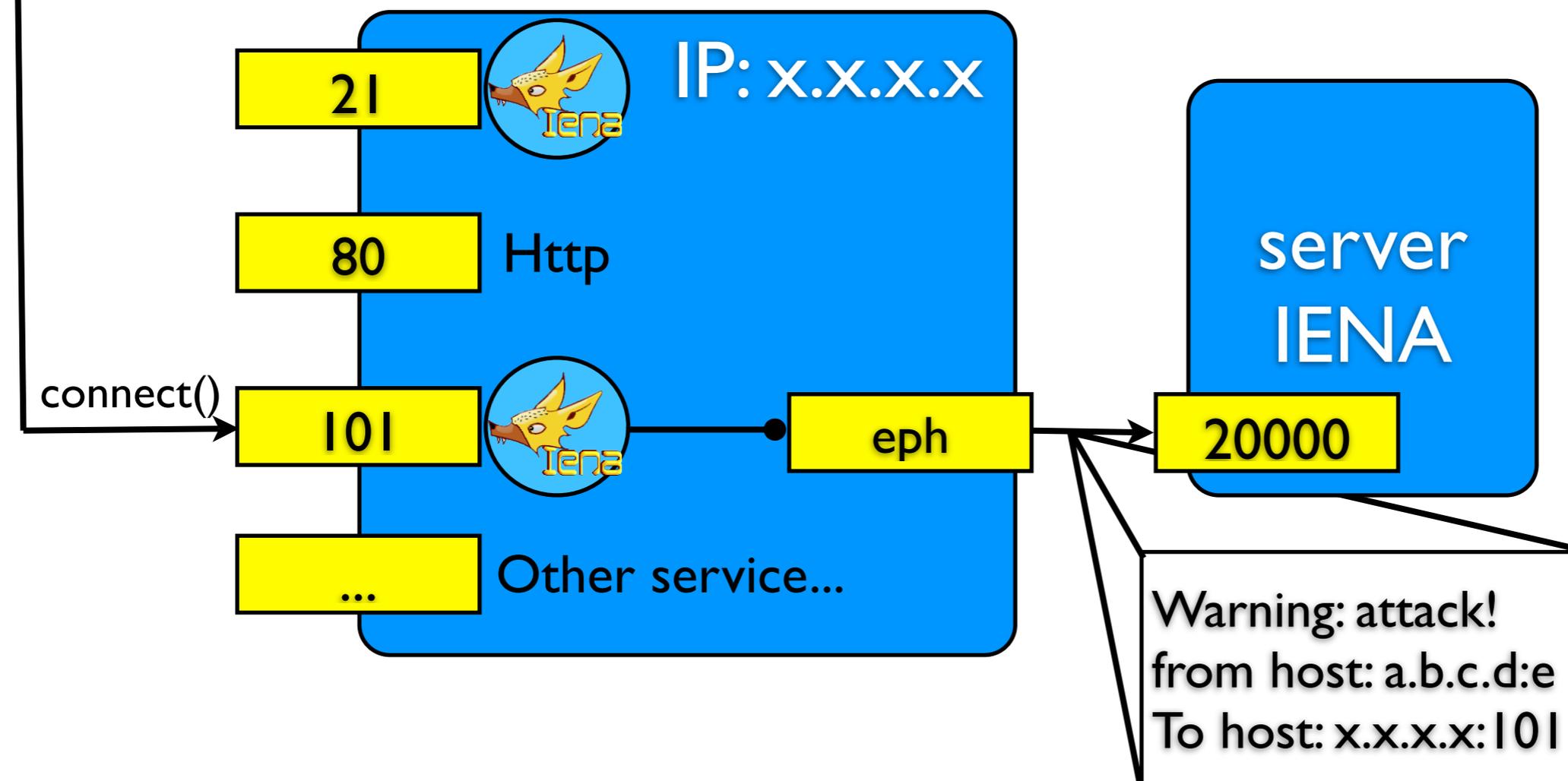


# IENA: comportamento



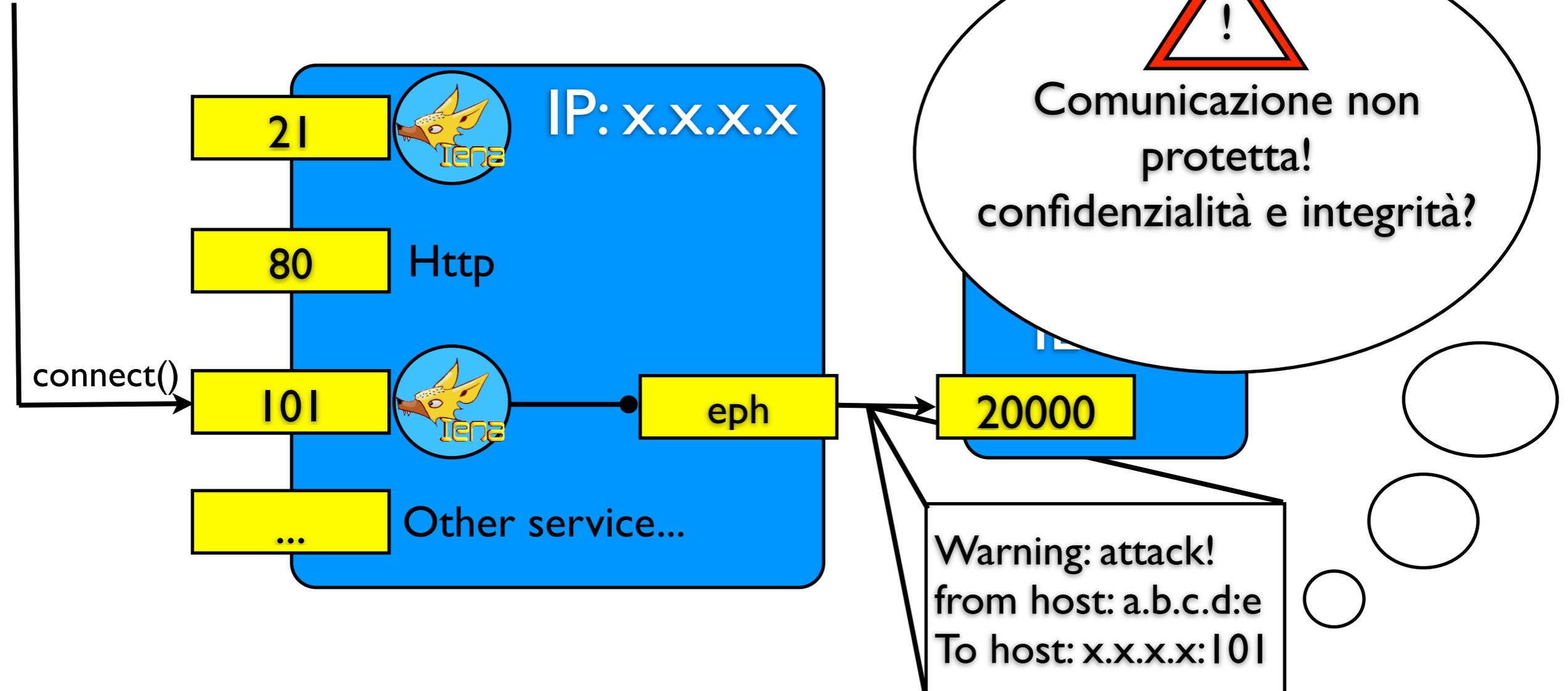
# Come vengono rilevati gli attacchi?

Attacker  
IP: a.b.c.d:e



# Come vengono rilevati gli attacchi?

Attacker  
IP: a.b.c.d:e



# Estensione del progetto

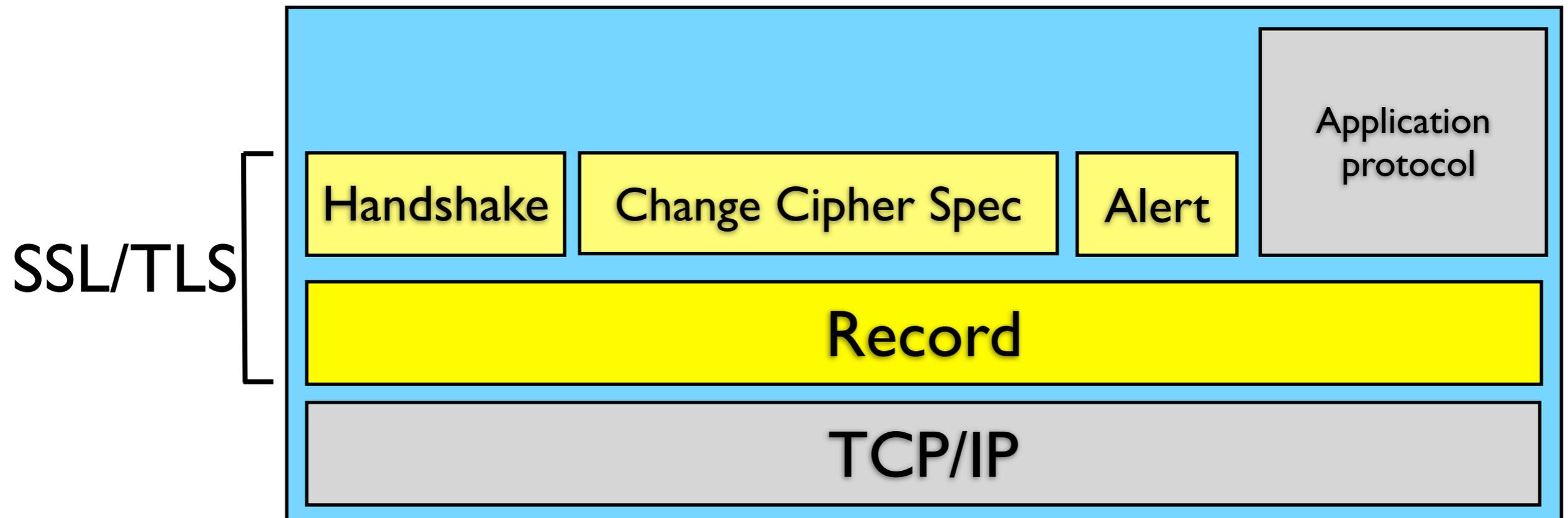
## PRIMA IMPLEMENTAZIONE

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

## PRIMA ESTENSIONE

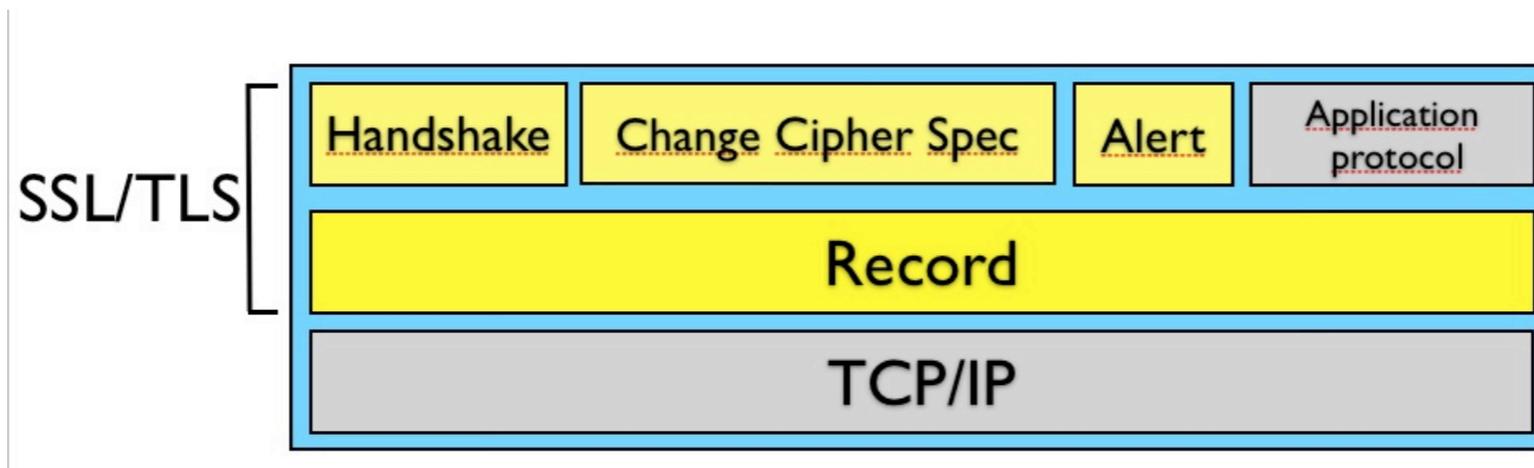
- ★ serverIENA (Java) + log su file;
- clientIENA (Java);
- ★ Comunicazione client/server protetta: SSL/TLS (mutual authentication)

# Secure Socket Layer (SSL)



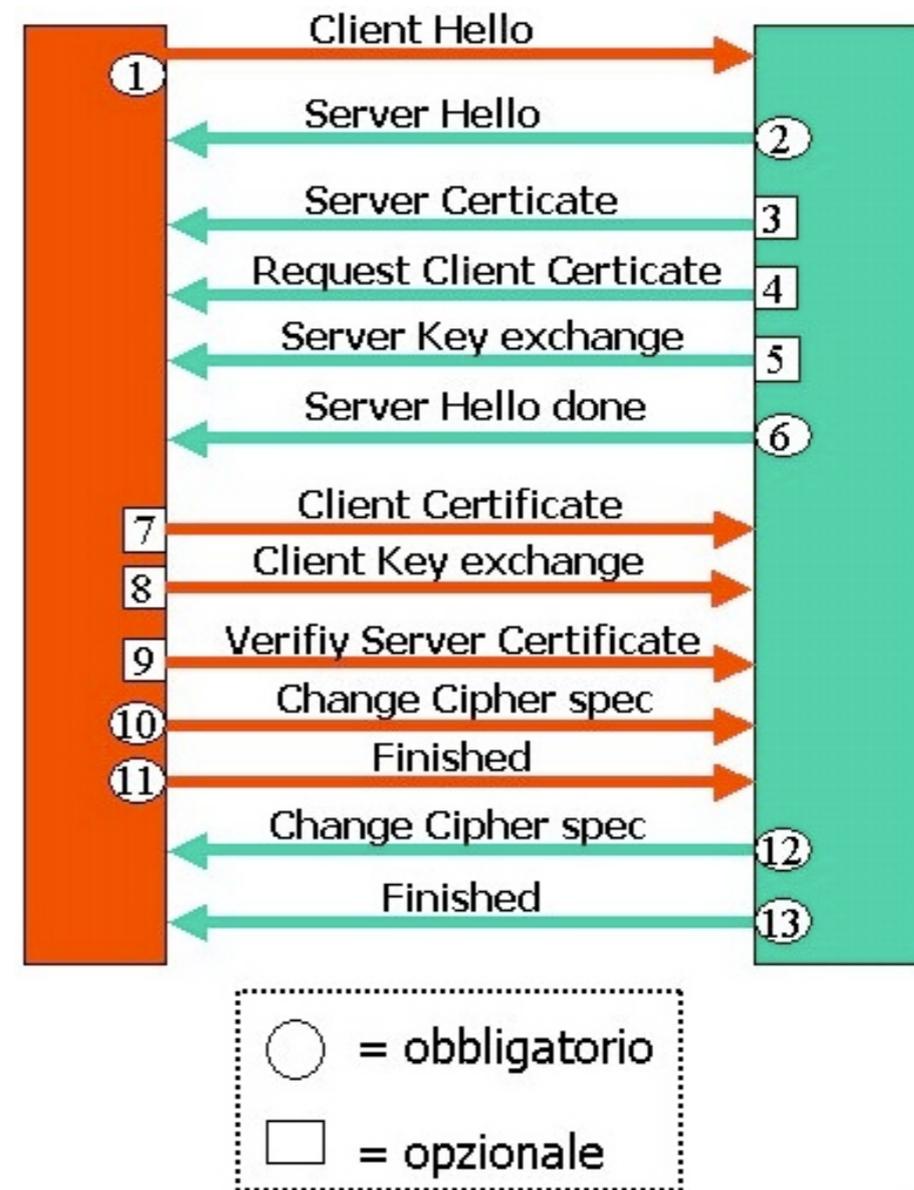
# SSL: sub-protocols

- 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]:**  
SSLvx.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.

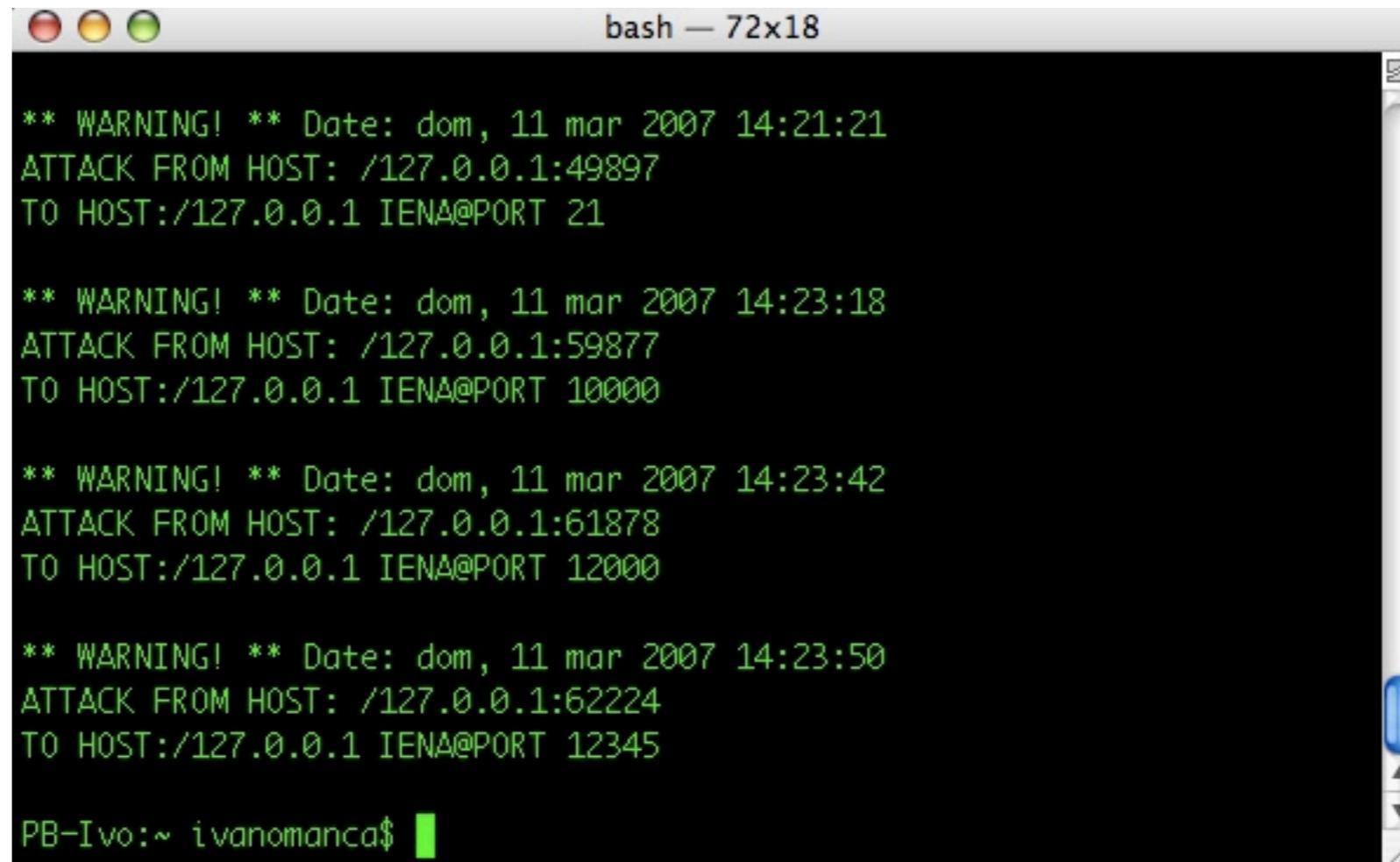
# Simulazione attacco

- ★ 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!

A terminal window titled "bash — 72x18" showing four log entries from the IENA firewall. Each entry starts with "\*\* WARNING! \*\*", followed by the date and time, the source host and port, and the destination host and port. The logs show attacks from 127.0.0.1 to IENA@PORT 21, 10000, 12000, and 12345.

```
bash — 72x18
** WARNING! ** Date: dom, 11 mar 2007 14:21:21
ATTACK FROM HOST: /127.0.0.1:49897
TO HOST:/127.0.0.1 IENA@PORT 21

** WARNING! ** Date: dom, 11 mar 2007 14:23:18
ATTACK FROM HOST: /127.0.0.1:59877
TO HOST:/127.0.0.1 IENA@PORT 10000

** WARNING! ** Date: dom, 11 mar 2007 14:23:42
ATTACK FROM HOST: /127.0.0.1:61878
TO HOST:/127.0.0.1 IENA@PORT 12000

** WARNING! ** Date: dom, 11 mar 2007 14:23:50
ATTACK FROM HOST: /127.0.0.1:62224
TO HOST:/127.0.0.1 IENA@PORT 12345

PB-Ivo:~ ivanomanca$
```

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

Applicazioni Risorse Sistema mar 6 mar, 12.25

ienachiaro.cap - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter:  + Expression... Pulisci Applica

No. .	Time	Source	Destination	Protocol	Info
6	0.022218	127.0.0.1	127.0.0.1	TCP	49551 > www [FIN, ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM : 0x0000]
7	0.022287	127.0.0.1	127.0.0.1	TCP	www > 49551 [ACK] Seq=1 Ack=2 Win=65535 [TCP CHECKSUM : 0x0000]
8	0.022383	127.0.0.1	127.0.0.1	TCP	49553 > 81 [SYN] Seq=0 [TCP CHECKSUM INCORRECT] Len=0
9	0.022413	127.0.0.1	127.0.0.1	TCP	81 > 49553 [RST, ACK] Seq=0 Ack=1 Win=0 [TCP CHECKSUM : 0x0000]
10	0.054812	127.0.0.1	127.0.0.1	TCP	49552 > 20000 [SYN] Seq=0 [TCP CHECKSUM INCORRECT] Len=0
11	0.054910	127.0.0.1	127.0.0.1	TCP	20000 > 49552 [SYN, ACK] Seq=0 Ack=1 Win=65535 [TCP CHECKSUM : 0x0000]
12	0.054932	127.0.0.1	127.0.0.1	TCP	49552 > 20000 [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM : 0x0000]
13	0.432029	127.0.0.1	127.0.0.1	DNP 3.0	len=84, from 17952 to 19267, Reset of User Process
14	0.432103	127.0.0.1	127.0.0.1	TCP	20000 > 49552 [ACK] Seq=1 Ack=50 Win=65535 [TCP CHECKSUM : 0x0000]
15	0.432305	127.0.0.1	127.0.0.1	TCP	49552 > 20000 [FIN, ACK] Seq=50 Ack=1 Win=65535 [TCP CHECKSUM : 0x0000]
16	0.432349	127.0.0.1	127.0.0.1	TCP	20000 > 49552 [ACK] Seq=1 Ack=51 Win=65535 [TCP CHECKSUM : 0x0000]

Window size: 65535  
Checksum: 0xfe59 [incorrect, should be 0xbd95]

Options: (12 bytes)

▼ Distributed Network Protocol 3.0

- ▶ Data Link Layer, Len: 84, From: 17952, To: 19267, PRM, Reset of User Process
- ▶ Transport Layer: 0x4d (FIR, Sequence 13)  
CRC failed, 0 chunks

```
0000 00 00 00 02 45 00 00 65 5c 6d 40 00 40 06 00 00  ....E..e \m@.@...
0010 7f 00 00 01 7f 00 00 01 c1 90 4e 20 5e 14 c4 b0  ..... ..N ^...
0020 da ed 66 90 80 18 ff ff fe 59 00 00 01 01 08 0a  ..f..... .Y.....
0030 4e 5e 0c b8 4e 5e 0c b8 41 54 54 41 43 4b 20 46  N^..N^.. ATTACK F
0040 52 4f 4d 20 2f 31 32 37 2e 30 2e 30 2e 31 3a 34  ROM /127 .0.0.1:4
0050 39 35 35 31 20 2d 2d 54 4f 2d 2d 3e 20 49 45 4e  9551 --T 0--> IEN
0060 41 40 50 4f 52 54 20 38 30 40 50 4f 52 54 20 38  A@PORT 8 0
```

Distributed Network Protocol 3.0 (dnp3), 49 bytes P: 18 D: 18 M: 0

ienachiaro.cap - Ethereal

# Estensione: connessione sicura (SSL/TLS)

The screenshot shows the Wireshark interface with a capture of a Distributed Network Protocol 3.0 (DNP3) packet. The packet list pane shows several packets, with packet 12 highlighted in red, indicating an error. The packet details pane shows the TCP header with a red highlight on the checksum field: "Checksum: 0xfeaa [incorrect, should be 0x8ffd]". The packet bytes pane shows the raw data of the packet, with a blue highlight on the payload area.

No.	Time	Source	Destination	Protocol	Info
9	0.076222	127.0.0.1	127.0.0.1	TCP	49541 > www [FIN, ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM : ]
10	0.076292	127.0.0.1	127.0.0.1	TCP	www > 49541 [ACK] Seq=1 Ack=2 Win=65535 [TCP CHECKSUM : ]
11	0.076388	127.0.0.1	127.0.0.1	TCP	49543 > 81 [SYN] Seq=0 [TCP CHECKSUM INCORRECT] Len=0 [ ]
12	0.076421	127.0.0.1	127.0.0.1	TCP	81 > 49543 [RST, ACK] Seq=0 Ack=1 Win=0 [TCP CHECKSUM : ]
13	0.077940	127.0.0.1	127.0.0.1	DNP 3.0	len=1, from 0 to 381, ACK
14	0.077995	127.0.0.1	127.0.0.1	TCP	20000 > 49542 [ACK] Seq=1 Ack=131 Win=65535 [TCP CHECKSUM : ]
15	0.099114	127.0.0.1	127.0.0.1	DNP 3.0	len=1, from 0 to 586, ACK
16	0.099176	127.0.0.1	127.0.0.1	TCP	49542 > 20000 [ACK] Seq=131 Ack=80 Win=65535 [TCP CHECKSUM : ]
17	0.099777	127.0.0.1	127.0.0.1	DNP 3.0	[Unreassembled Packet [incorrect TCP checksum]]

Flags: 0x0018 (PSH, ACK)  
Window size: 65535  
Checksum: 0xfeaa [incorrect, should be 0x8ffd]  
Options: (12 bytes)

Distributed Network Protocol 3.0  
Data Link Layer, Len: 1, From: 0, To: 381, ACK

```
0000 00 00 00 02 45 00 00 b6 59 1d 40 00 40 06 00 00 ....E... Y.@.@...
0010 7f 00 00 01 7f 00 00 01 c1 86 4e 20 53 1b 56 c2 ..... ..N S.V.
0020 ab b8 9c 59 80 18 ff ff fe aa 00 00 01 01 08 0a ...Y....
0030 4e 5e 09 09 4e 5e 09 09 16 03 01 00 7d 01 00 00 N^..N^.. ....}...
0040 79 03 01 45 dc 6c 4b f7 39 cb 7e a2 fe 6a a3 f9 y..E.lK. 9~.j..
0050 9a 2d 29 00 d6 77 a7 cb fa 6e d3 d9 8d c3 4b d7 .-)..w.. .n...K.
0060 8c 49 72 20 45 dc 6a c2 f8 9d 93 69 8f fb 66 7d .Ir E.j. ...i..f}
0070 d3 63 04 35 cd e7 c1 5c 24 3e a1 39 15 33 84 00 .c.5...\ $>.9.3..
0080 ce 56 f3 99 00 32 00 04 00 05 00 2f 00 35 00 33 .V...2.. .../.5.3
0090 00 39 00 32 00 38 00 0a 00 16 00 13 00 09 00 15 .9.2.8..
00a0 00 12 00 03 00 08 00 14 00 11 00 18 00 34 00 3a .....4.:
00b0 00 1b 00 1a 00 17 00 19 01 00 .....
```

Distributed Network Protocol 3.0 (dnp3), 130 bytes P: 34 D: 34 M: 0

# Autenticazione clientIENA/serverIENA

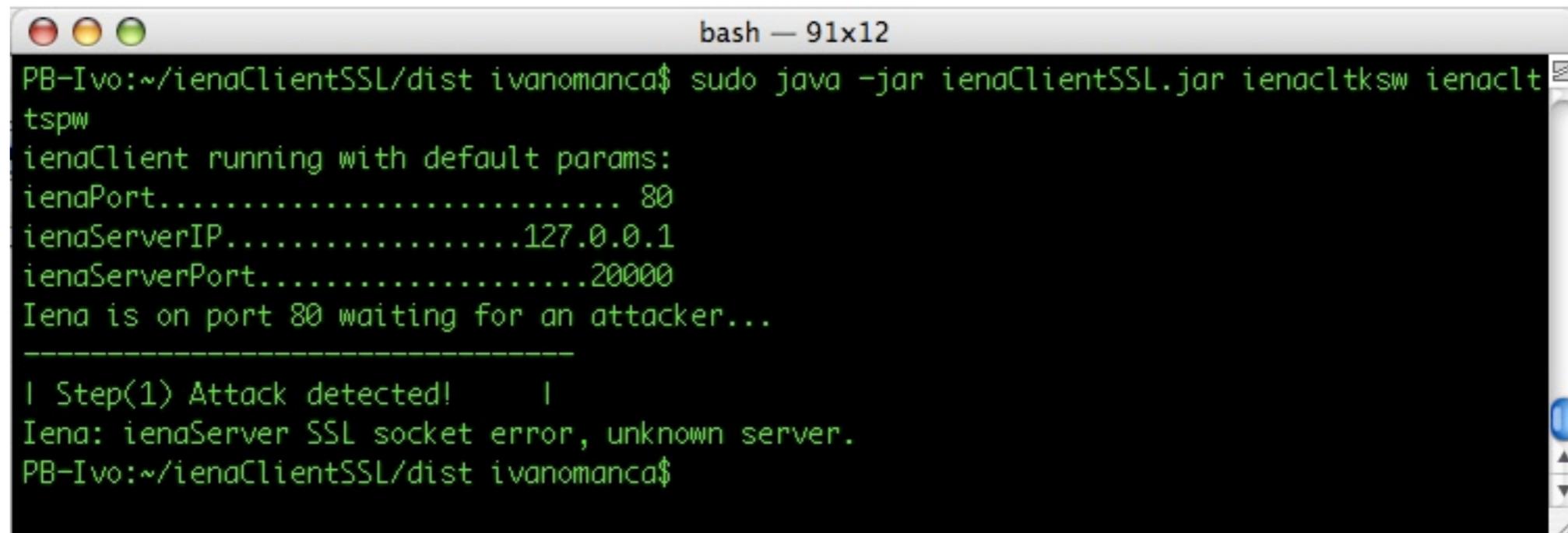
- Un client qualsiasi tenta una connessione al serverIENA...



```
java — 84x6
PB-Ivo:~/ienaServerSSL/dist ivanomanca$ java -jar ienaServerSSL.jar ienasrvkspw
ienaServer running with default params:
ienaServerPort.....20000
ienaServer running on port: 20000
Warning: connection failed, unknown client refused.
```

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

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



```
bash — 91x12
PB-Ivo:~/ienaClientSSL/dist ivanomanca$ sudo java -jar ienaClientSSL.jar ienacltksw ienaclt
tspw
ienaClient running with default params:
ienaPort..... 80
ienaServerIP.....127.0.0.1
ienaServerPort.....20000
Iena is on port 80 waiting for an attacker...
-----
| Step(1) Attack detected!      |
Iena: ienaServer SSL socket error, unknown server.
PB-Ivo:~/ienaClientSSL/dist ivanomanca$
```

...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”).