Università della Svizzera italiana

Advanced Learning and Research Institute ALaRI

Ma il software open source è sicuro?

Alberto Ferrante
ALaRI, Facoltà di Informatica
Università della Svizzera italiana
E-mail: ferrante@alari.ch

Sommario

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Conclusioni

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Conclusioni

E la qualità del codice?
Chi scrive il software OS?
Sviluppo
La realtà
Ma se tutti possono vedere il codice ...
Una tecnologia per la sicurezza
Conclusioni

Parliamo della qualità del codice?

Chi scrive il software OS?

E la qualità del codice?
Chi scrive il software OS?
Sviluppo
La realtà
Ma se tutti possono vedere il codice ...
Una tecnologia per la sicurezza
Conclusioni

La qualità del codice è variabile:

- ✔ ad ogni progetto possono contribuire diverse persone;
- ✔ non sempre la qualità del codice prodotto è sufficiente;
- ✔ non c'è validazione.

Chi scrive il software OS?

E la qualità del codice?
Chi scrive il software OS?
Sviluppo
La realtà
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Conclusioni

La qualità del codice è variabile:

- ✔ ad ogni progetto possono contribuire diverse persone;
- ✔ non sempre la qualità del codice prodotto è sufficiente;
- ✔ non c'è validazione.

. . . Ma è davvero così?

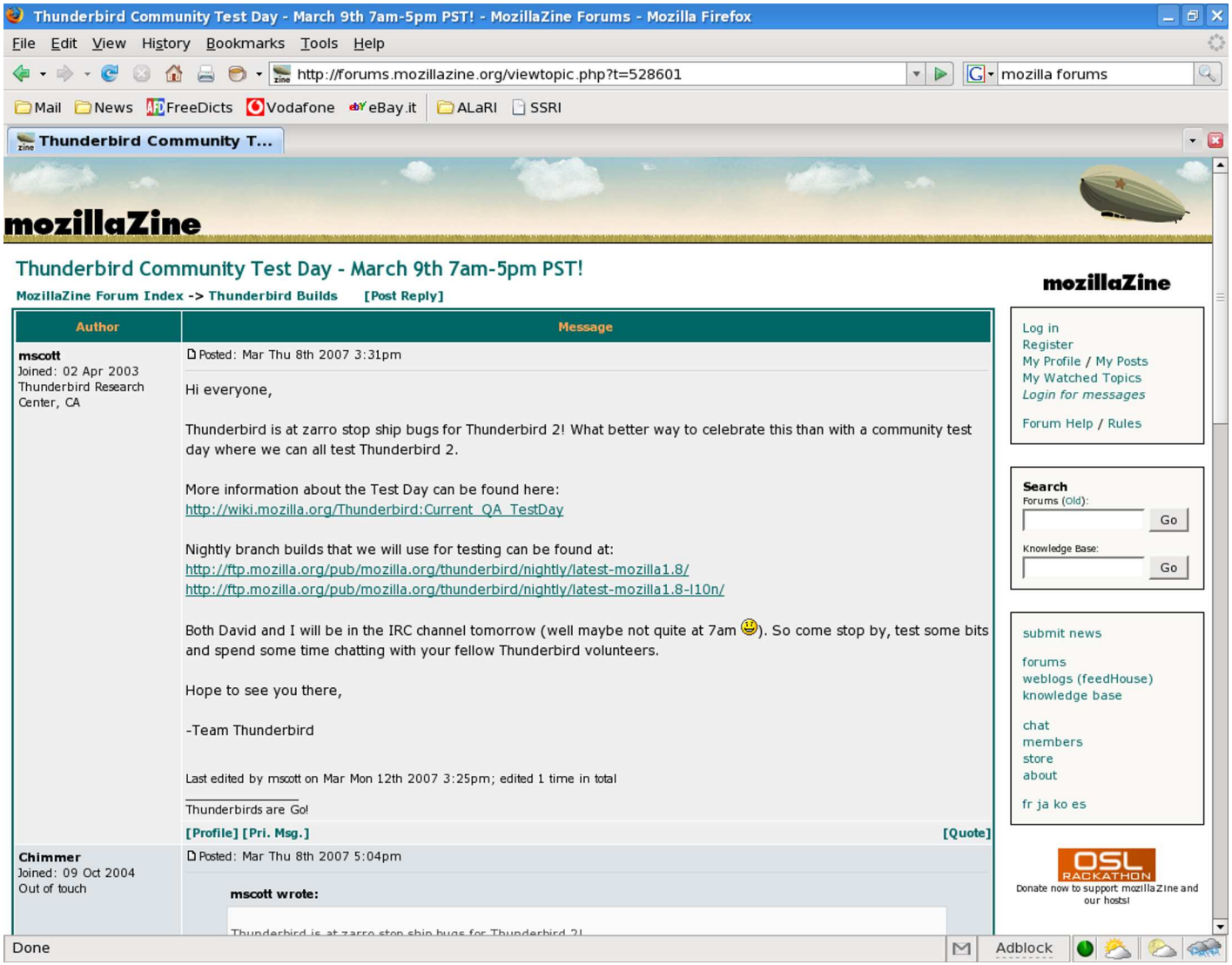
Lo sviluppo (1/2)

E la qualità del codice?
Chi scrive il software OS?
Sviluppo
La realtà
Ma se tutti possono vedere il codice ...
Una tecnologia per la sicurezza
Conclusioni

- ✔ Ogni progetto OS è diverso;
- ✔ meccanismi di controllo della qualità;
- ✔ numero di "beta tester" elevato:
  - ✘ testing pubblico del codice sviluppato;
  - ✘ sistemi di bug-tracking efficienti.

Lo sviluppo (1/2)

E la qualità del codice?
Chi scrive il software OS?
Sviluppo
La realtà
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Conclusioni



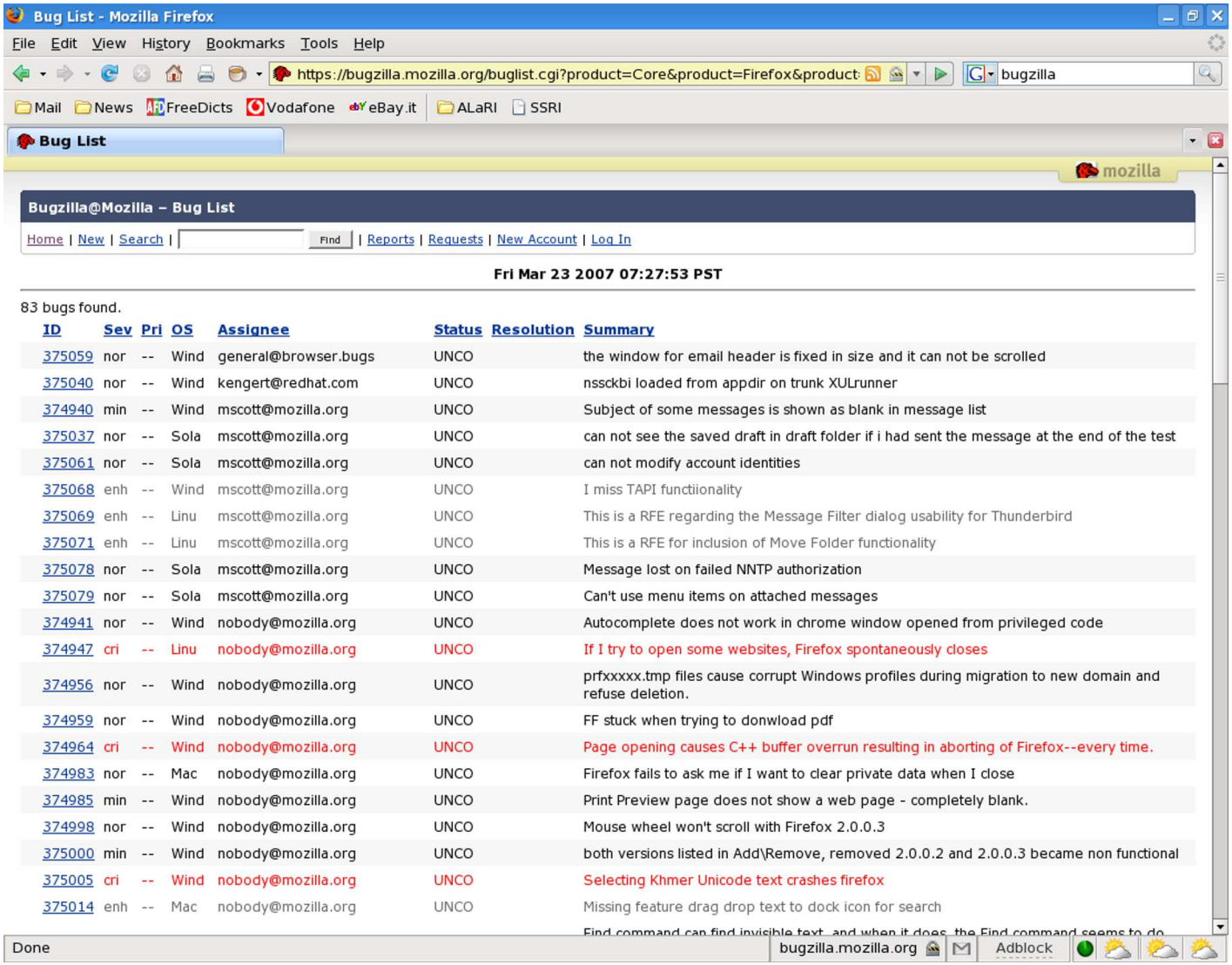
Lo sviluppo (1/2)

E la qualità del codice?
Chi scrive il software OS?
Sviluppo
La realtà
Ma se tutti possono vedere il codice ...
Una tecnologia per la sicurezza
Conclusioni

- ✔ Ogni progetto OS è diverso;
- ✔ meccanismi di controllo della qualità;
- ✔ numero di "beta tester" elevato:
  - ✘ testing pubblico del codice sviluppato;
  - ✘ sistemi di bug-tracking efficienti.

Lo sviluppo (1/2)

E la qualità del codice?
Chi scrive il software OS?
Sviluppo
La realtà
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Conclusioni



Lo sviluppo (2/2)

E la qualità del codice?
Chi scrive il software OS?
Sviluppo
La realtà
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Conclusioni

- ✔ non ci sono scadenze commerciali:
  - ✘ release ritardate per bug importanti.

La realtà

E la qualità del codice?
Chi scrive il software OS?
Sviluppo
La realtà
Ma se tutti possono vedere il codice ...
Una tecnologia per la sicurezza
Conclusioni

In generale la qualità è comparabile
o superiore a quella di prodotti non OS.

Reasoning:
"The open-source implementation of TCP/IP in the Linux kernel clearly exhibits a higher code quality than commercial implementations in general-purpose operating systems" [1]

[1] Stephen Shankland, "Study lauds open-source code quality," available: http://news.com.com/2100-1001-985221.html

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Svantaggi
Vantaggi
Un esempio
Una tecnologia per la sicurezza
Conclusioni

. . . Ma se tutti possono vedere il codice. . .

Il codice è pubblico: svantaggi

E la qualità del codice?
Ma se tutti possono vedere il codice ...
Svantaggi
Vantaggi
Un esempio
Una tecnologia per la sicurezza
Conclusioni

La disponibilità del codice sorgente rende il sistema vulnerabile:

- ✔ potendo vedere il codice è più facile scoprirne le debolezze!

Il codice è pubblico: svantaggi

E la qualità del codice?
Ma se tutti possono vedere il codice ...
Svantaggi
Vantaggi
Un esempio
Una tecnologia per la sicurezza
Conclusioni

La disponibilità del codice sorgente rende il sistema vulnerabile:

✔ potendo vedere il codice
è più facile scoprirne le debolezze!

...Ma è davvero così?

Il codice è pubblico: vantaggi

E la qualità del codice?
Ma se tutti possono vedere il codice ...
Svantaggi
Vantaggi
Un esempio
Una tecnologia per la sicurezza
Conclusioni

- ✔ La disponibilità del codice sorgente permette di scoprire prima i difetti;
- ✔ le vulnerabilità possono essere trovate anche non avendo a disposizione il codice.

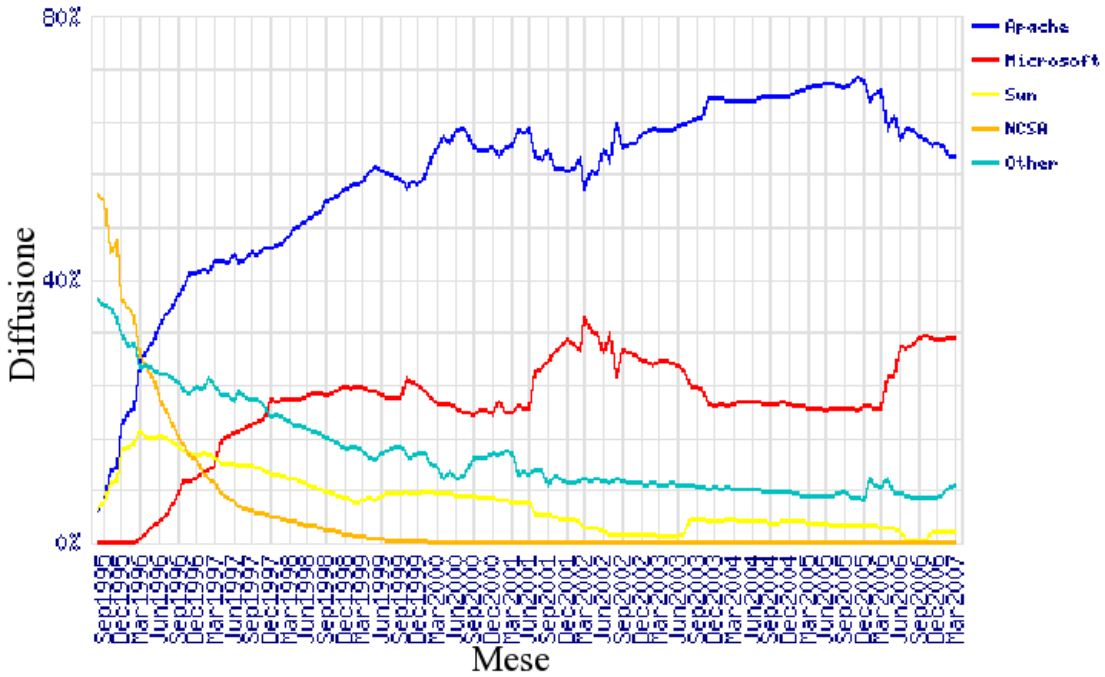
Un vantaggio importante

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Svantaggi
Vantaggi
Un esempio
Una tecnologia per la sicurezza
Conclusioni

- ✔ Il software OS può essere analizzato da tutti:
  - ✘ **certezza che il prodotto faccia solo quello che deve e non altro!**

Un esempio: il web server Apache

E la qualità del codice?
Ma se tutti possono vedere il codice ...
Svantaggi
Vantaggi
Un esempio
Una tecnologia per la sicurezza
Conclusioni



[2]

- ✔ progetto open source;
- ✔ considerato uno dei più sicuri.

[2] Netcraft. http://news.netcraft.com

"The necessity of operating system security to overall system security is undeniable... If it fails to meet this responsibility, system-wide vulnerabilities will result"
[3, pag. 4].

[3] Frank Mayer, Karl Macmillan, and David Caplan, *SELinux by Example*. Prentice Hall, 2007

Una tecnologia OS per la sicurezza

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Una tecnologia OS per la sicurezza
SELinux: come funziona
SELinux: a cosa serve?
SELinux: dove lo troviamo?
SELinux: problemi
Conclusioni

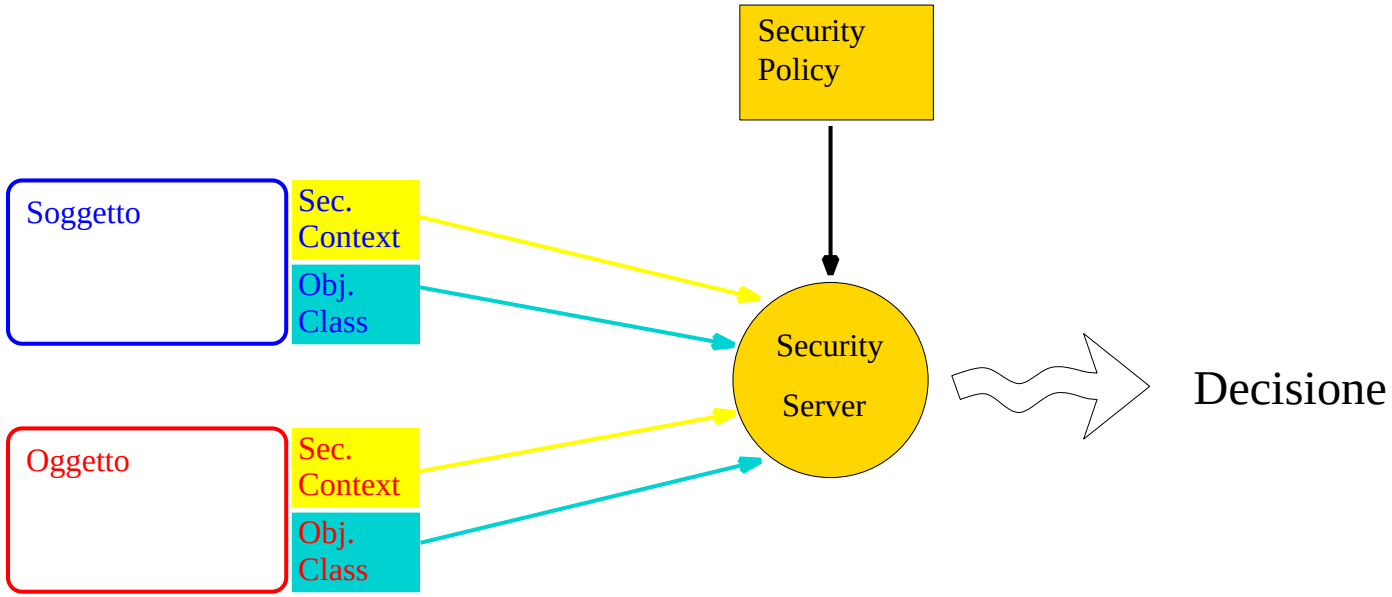
SELinux [4, 5]:

- ✔ sviluppato dalla NSA;
- ✔ nuovo standard di sicurezza per i sistemi operativi;
- ✔ mitiga il problema dei buchi di sicurezza delle applicazioni;
- ✔ *Mandatory Access Control* flessibile.

[4] NSA security enhanced linux. http://www.nsa.gov/selinux
[5] Stephen Smalley, *Configuring the SELinux Policy*, NSA, Feb. 2005

SELinux:come funziona

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Una tecnologia OS per la sicurezza
SELinux: come funziona
SELinux: a cosa serve?
SELinux: dove lo troviamo?
SELinux: problemi
Conclusioni



- ✔ *soggetti*: processi;
- ✔ *oggetti*: file, canali di comunicazione tra processi, socket, host, . . .

SELinux: security server

E la qualità del codice?
Ma se tutti possono vedere il codice ...
Una tecnologia per la sicurezza
Una tecnologia OS per la sicurezza
SELinux: come funziona
SELinux: a cosa serve?
SELinux: dove lo troviamo?
SELinux: problemi
Conclusioni

- ✔ Nel kernel;
- ✔ diverse implementazioni possibili con la stessa architettura di sistema;
  - ✘ l'attuale unisce:
    - ✓ Type Enforcement;
    - ✓ Role Based Access Control;
    - ✓ Multi-level Security.

SELinux: a cosa serve?

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Una tecnologia OS per la sicurezza
SELinux: come funziona
SELinux: a cosa serve?
SELinux: dove lo troviamo?
SELinux: problemi
Conclusioni

- ✔ Accesso consentito
  solo a parti predeterminate del sistema;
- ✔ consentite solo le azioni
  strettamente necessarie al funzionamento.

SELinux: a cosa serve?

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Una tecnologia OS per la sicurezza
SELinux: come funziona
SELinux: a cosa serve?
SELinux: dove lo troviamo?
SELinux: problemi
Conclusioni

- ✔ Accesso consentito
  solo a parti predeterminate del sistema;
- ✔ consentite solo le azioni
  strettamente necessarie al funzionamento.

I servizi vengono “confinati”:
possono svolgere solo
le azioni specificate nella SELinux policy!

SELinux: dove lo troviamo?

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Una tecnologia OS per la sicurezza
SELinux: come funziona
SELinux: a cosa serve?
SELinux: dove lo troviamo?
SELinux: problemi
Conclusioni

- ✔ Parti fondamentali incluse nei kernel Linux dalla serie 2.6;
- ✔ distribuzioni Linux:
  - ✘ Red Hat (da Fedora Core 2 in poi);
  - ✘ Debian;
  - ✘ Yellow Dog Linux;
  - ✘ Hardened Gentoo.

SELinux: problemi

E la qualità del codice?
Ma se tutti possono vedere il codice ...
Una tecnologia per la sicurezza
Una tecnologia OS per la sicurezza
SELinux: come funziona
SELinux: a cosa serve?
SELinux: dove lo troviamo?
SELinux: problemi
Conclusioni

- ✔ Bisogna comprendere a fondo il meccanismo per configurarlo correttamente:
  - ✘ nelle distribuzioni:
    - ✓ policy già pronte molto buone;
    - ✓ difficili da customizzare.

Conclusioni (1/2)

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Conclusioni

- ✔ Il software OS **non è** intrinsecamente **meno sicuro** di quello non open;
- ✔ il software OS **non è** intrinsecamente **più sicuro** di quello non open;

Conclusioni (2/2)

E la qualità del codice?
Ma se tutti possono vedere il codice . . .
Una tecnologia per la sicurezza
Conclusioni

- ✔ la disponibilità del codice sorgente dà dei vantaggi;
- ✔ disponibilità di tecnologie per migliorare la sicurezza.

Ringrazio per l'attenzione . . .

E-mail: ferrante@alari.ch

Presentazione disponibile su:
http://www.alari.ch/people/alberto/publicationsframe.htm