

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

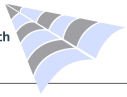
Conclusioni

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

The screenshot shows a MozillaZine forum thread titled "Thunderbird Community Test Day - March 9th 7am-5pm PST!". The post is by user "mscott" and discusses the upcoming test day for Thunderbird 2.0. It includes links to a wiki page for test day information and FTP links for nightly builds. A second user, "Chimmer", has replied with a quote of the original post.

Author	Message
mscott Joined: 02 Apr 2003 Thunderbird Research Center, CA	Posted: Mar Thu 8th 2007 3:31pm Hi everyone, Thunderbird is at zarro stop ship bugs for Thunderbird 2! What better way to celebrate this than with a community test day where we can all test Thunderbird 2. More information about the Test Day can be found here: http://wiki.mozilla.org/Thunderbird:Current_QA_TestDay Nightly branch builds that we will use for testing can be found at: http://ftp.mozilla.org/pub/mozilla.org/thunderbird/nightly/latest-mozilla1.8/ http://ftp.mozilla.org/pub/mozilla.org/thunderbird/nightly/latest-mozilla1.8-110n/ Both David and I will be in the IRC channel tomorrow (well maybe not quite at 7am 😊). So come stop by, test some bits and spend some time chatting with your fellow Thunderbird volunteers. Hope to see you there, -Team Thunderbird Last edited by mscott on Mar Mon 12th 2007 3:25pm; edited 1 time in total Thunderbirds are Go! [Profile] [Pri. Msg.] [Quote]
Chimmer Joined: 09 Oct 2004 Out of touch	Posted: Mar Thu 8th 2007 5:04pm mscott wrote: Thunderbird is at zarro stop ship bugs for Thunderbird 2!

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

83 bugs found.

ID	Sev	Pri	OS	Assignee	Status	Resolution	Summary
375059	nor	--	Wind	general@browser.bugs	UNCO		the window for email header is fixed in size and it can not be scrolled
375040	nor	--	Wind	kengert@redhat.com	UNCO		nssckbi loaded from appdir on trunk XULrunner
374940	min	--	Wind	mccott@mozilla.org	UNCO		Subject of some messages is shown as blank in message list
375037	nor	--	Sola	mccott@mozilla.org	UNCO		can not see the saved draft in draft folder if i had sent the message at the end of the test
375061	nor	--	Sola	mccott@mozilla.org	UNCO		can not modify account identities
375068	enh	--	Wind	mccott@mozilla.org	UNCO		I miss TAPI functionality
375069	enh	--	Linu	mccott@mozilla.org	UNCO		This is a RFE regarding the Message Filter dialog usability for Thunderbird
375071	enh	--	Linu	mccott@mozilla.org	UNCO		This is a RFE for inclusion of Move Folder functionality
375078	nor	--	Sola	mccott@mozilla.org	UNCO		Message lost on failed NNTP authorization
375079	nor	--	Sola	mccott@mozilla.org	UNCO		Can't use menu items on attached messages
374941	nor	--	Wind	nobody@mozilla.org	UNCO		Autocomplete does not work in chrome window opened from privileged code
374947	cri	--	Linu	nobody@mozilla.org	UNCO		If I try to open some websites, Firefox spontaneously closes
374956	nor	--	Wind	nobody@mozilla.org	UNCO		prfxxxx.tmp files cause corrupt Windows profiles during migration to new domain and refuse deletion.
374959	nor	--	Wind	nobody@mozilla.org	UNCO		FF stuck when trying to download pdf
374964	cri	--	Wind	nobody@mozilla.org	UNCO		Page opening causes C++ buffer overrun resulting in aborting of Firefox--every time.
374983	nor	--	Mac	nobody@mozilla.org	UNCO		Firefox fails to ask me if I want to clear private data when I close
374985	min	--	Wind	nobody@mozilla.org	UNCO		Print Preview page does not show a web page - completely blank.
374998	nor	--	Wind	nobody@mozilla.org	UNCO		Mouse wheel won't scroll with Firefox 2.0.0.3
375000	min	--	Wind	nobody@mozilla.org	UNCO		both versions listed in Add/Remove, removed 2.0.0.2 and 2.0.0.3 became non functional
375005	cri	--	Wind	nobody@mozilla.org	UNCO		Selecting Khmer Unicode text crashes firefox
375014	enh	--	Mac	nobody@mozilla.org	UNCO		Missing feature drag drop text to dock icon for search

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.

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

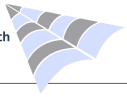
Conclusioni

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

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

E la qualità del codice?

Ma se tutti possono vedere il codice ...

Svantaggi

Vantaggi

Un esempio

Una tecnologia per la sicurezza

Conclusioni

Un esempio: il web server Apache

E la qualità del codice?

Ma se tutti possono vedere il codice ...

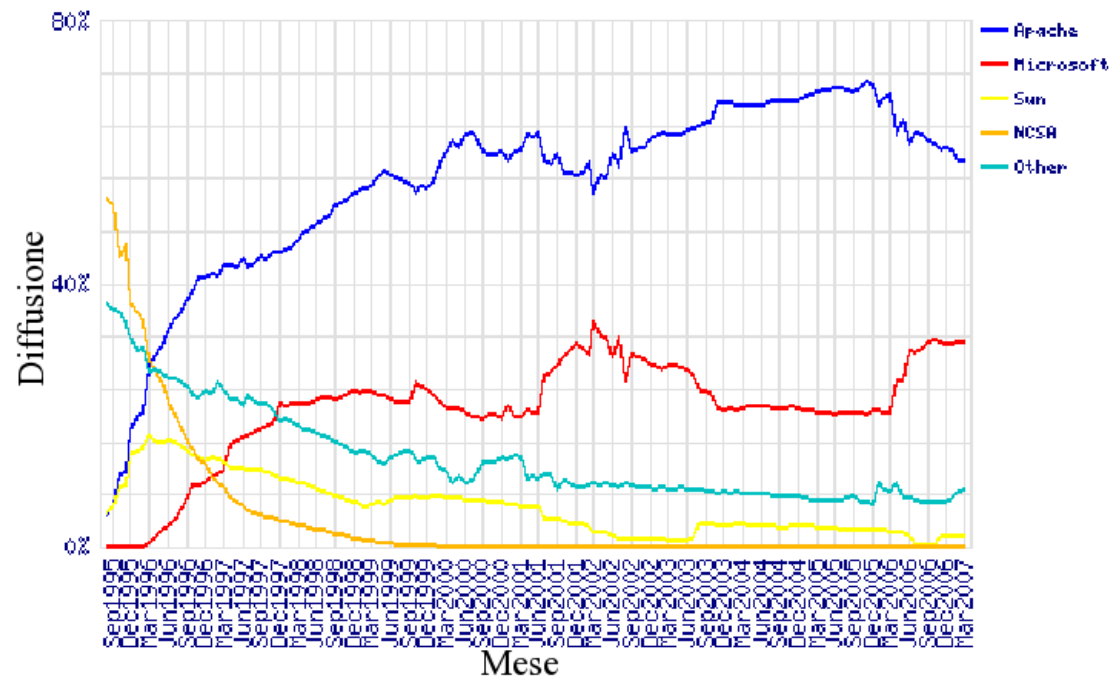
Svantaggi

Vantaggi

Un esempio

Una tecnologia per la sicurezza

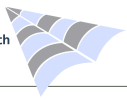
Conclusioni



[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

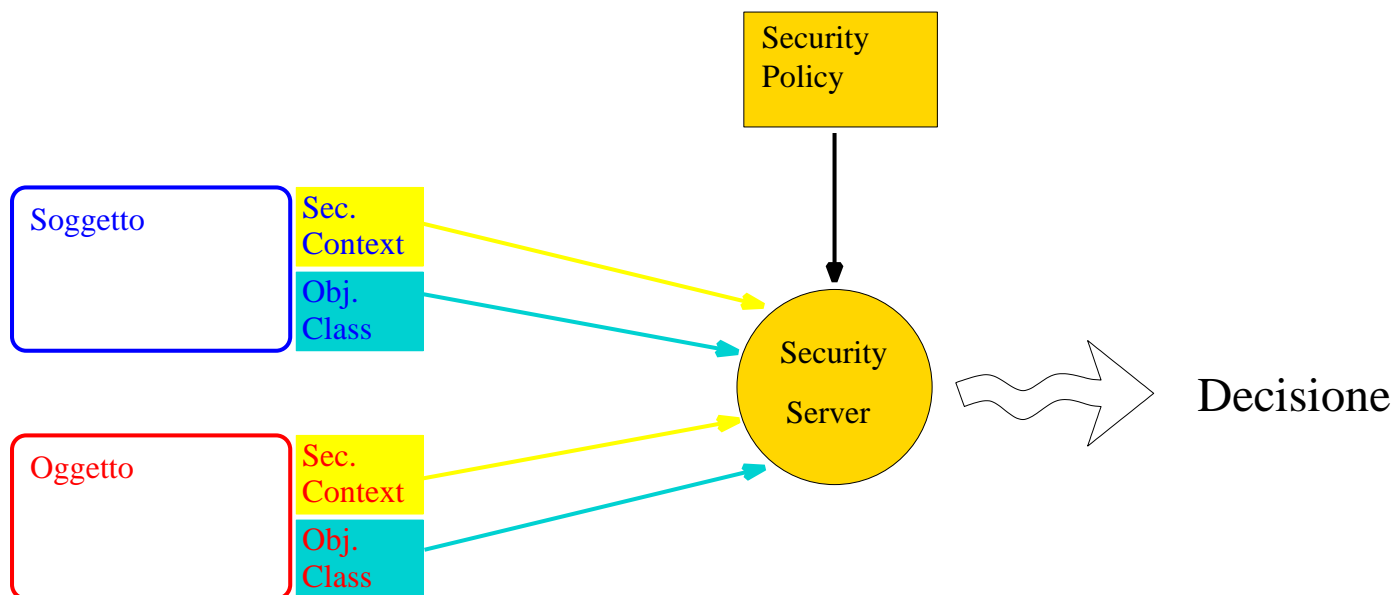
SELinux: come funziona

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>