YAK

Una proposta per gli accessi pubblici a Internet nelle biblioteche di Ateneo

Alberto Cammozzo*, Mauro Malvestio**

25/10/05, revisione 3

La recente normativa antiterrorismo impone misure severe per chi offre a vario titolo accesso a Internet al pubblico, aggravando le gia' serie problematiche legate alla sicurezza informatica. Le biblioteche universitarie, almeno a una prima analisi, cadono in questa categoria. Scienze Statistiche ha cercato di affrontare queste problematiche con una soluzione informatica non onerosa e il piu' possibile composta da software libero.

Il decreto antiterrorismo:

Il recente decreto antiterrorismo[1], e la sua conversione in legge[2] prevedono che (art.7)

> *chiunque intende aprire un pubblico esercizio o un circolo privato di qualsiasi specie la cui esclusiva o prevalente attivita' consista nel mettere a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, oppure in cui siano installati piu' di tre apparecchi terminali*

e' tenuto a adottare misure

> *per il monitoraggio delle operazioni dell'utente e per l'archiviazione dei relativi dati [...], nonche' misure di preventiva acquisizione di dati anagrafici riportati su un documento di identita' dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili.*

Le misure sono precisate e definite come segue nel decreto del Ministero dell'interno 16 agosto 2005[3]:

> *a) adottare le misure fisiche o tecnologiche occorrenti per impedire l'accesso agli apparecchi terminali a persone che non siano preventivamente identificate con le modalita' di cui alla lettera b);*
>
> *b) identificare chi accede ai servizi telefonici e telematici offerti, prima dell'accesso stesso o dell'offerta di credenziali di accesso, acquisendo i dati anagrafici riportati su un documento di identita', nonche' il tipo, il numero e la riproduzione del documento presentato dall'utente;*
>
> *c) adottare le misure di cui all'art. 2, occorrenti per il monitoraggio*

* Dipartimento di Scienze Statistiche, mmzz @ stat.unipd.it
** Biblioteca della Facolta' di Scienze Statistiche, malveo @ stat.unipd.it

1 http://gazzette.comune.jesi.an.it/2005/173/1.htm
2 http://gazzette.comune.jesi.an.it/2005/177/3.htm
3 http://www.giustizia.gov.it/cassazione/leggi/d16ago_05.html

delle attivita'; d) informare, anche in lingue straniere, il pubblico delle condizioni d'uso dei terminali messi a disposizione, comprese quelle di cui alle lettere a) e b);
e) rendere disponibili, a richiesta, anche per via telematica, i dati acquisiti a norma delle lettere b) e c), esclusi comunque i contenuti delle comunicazioni, al Servizio polizia postale e delle comunicazioni, quale organo del Ministero dell'interno preposto ai servizi di polizia postale e delle comunicazioni, nonche', in conformità al codice di procedura penale, all'autorita' giudiziaria e alla polizia giudiziaria;
f) assicurare il corretto trattamento dei dati acquisiti e la loro conservazione fino al 31 dicembre 2007.

L'art.3 comma 2 dello stesso decreto suggerisce che i terminali installati all'interno *di centri di ricerca, universita' ed altri istituti di istruzione* sono soggetti alla 155/05.

A completare il quadro viene la circolare del Ministero dell'interno n.557/2005[4].

La situazione delle biblioteche:

Servizi: le biblioteche universitarie, inclusa quella di Scienze Statistiche, solitamente offrono la possibilita' di accedere a dei PC connessi ad Internet per:
a) svolgere ricerche bibliografiche attraverso OPAC (all'interno alla rete di Ateneo),
b) svolgere ricerche in altri servizi o database interni alla rete di Ateneo,
c) svolgere ricerche attraverso la navigazione in Internet, anche fuori dalla rete di Ateneo.

Per quanto riguarda l'art.7 del decreto, i punti a) e b) non sono problematici, a condizione di mettere in atto misure che impediscono la navigazione all'esterno della rete di Ateneo (con un firewall perimetrale o dei personal firewall).
Benche' al momento non vi siano indicazioni precise, pare invece che per quanto riguarda il punto c) le biblioteche dovranno mettere in atto le misure previste dal decreto del Ministero dell'interno 16 agosto 2005 oppure vietare l'accesso ai computer da parte di utenti esterni.

Utenza: l'uso delle risorse informatiche rivolte al pubblico offerte delle Biblioteche prevede l'accesso da parte di:
a) studenti ed ex studenti,
b) personale docente e tecnico-amministrativo,
c) esterni.

Le *misure tecnologiche per l'accesso* richiedono che venga identificato ogni utente e ad esso vengano legate le attivita' svolte nella sua sessione di lavoro. Il modo piu' agevole e consolidato per ottenere questo scopo, specie per gli utenti abituali, e' assegnare delle credenziali (username e password) all'utente con le quali lasciarlo accedere ai PC. Le biblioteche hanno due possibilita':

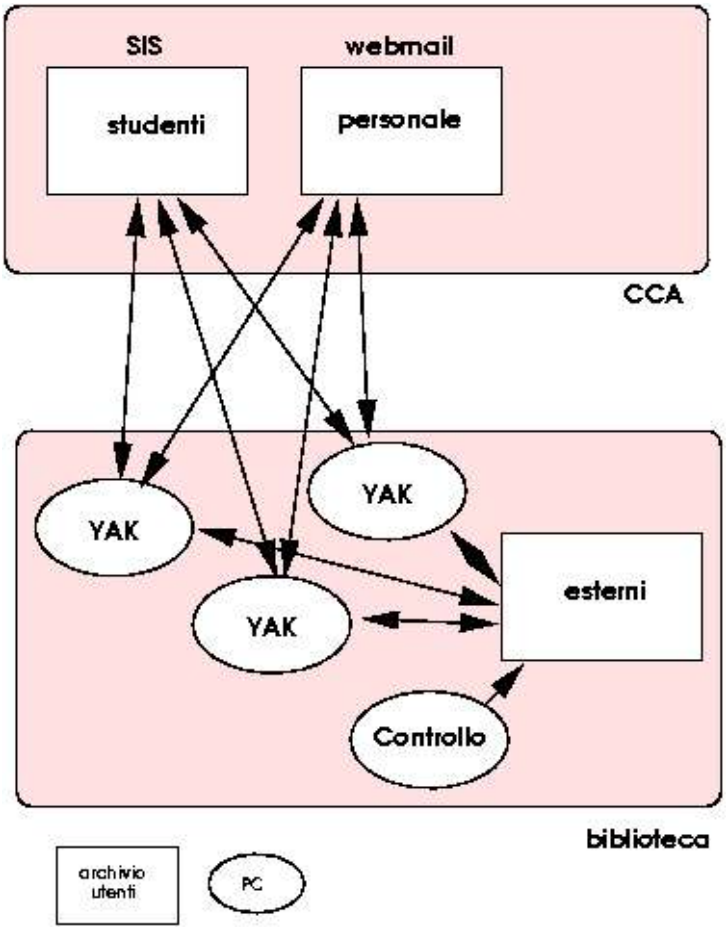
4 http://www.bn.camcom.it/html/news/43/Circolare%20Ministero%20dell'Interno%20557%20-%2005.pdf

1) Ogni biblioteca, indipendentemente, acquisisce i dati dei propri utenti e assegna ad essi le credenziali.
2) L'Ateneo offre alle biblioteche un servizio centralizzato per autenticare gli utenti che dispongono gia' di qualche altra credenziale a livello di Ateneo.

A quanto risulta, diverse biblioteche si sono dotate gia' di sistemi di tipo 1) reperibili sul mercato. L'Ateneo al momento non offre esplicitamente un servizio centralizzato di autenticazione (*Single Sign-on* di Ateneo) per realizzare sistemi di tipo 2).

La proposta

Pur non essendovi ancora un sistema di autenticazione centralizzata, esistono gia' dei servizi on-line presso il Centro di Calcolo di Ateneo rivolti alle categorie di utenti a) e b): il SIS[5] per gli studenti e il sistema di posta elettronica (webmail) di Ateneo[6] per il personale, sia docente che tecnico amministrativo (TA).



La Biblioteca di Scienze Statistiche, in collaborazione con i servizio SEAD/ASID del Dipartimento di Scienze Statistiche, ha avviato a titolo sperimentale un servizio di chioschi per l'accesso a Internet denominato YAK (*yet another kiosk*), che permette di autenticare le categorie a) e b)[7], basato su GNU/Linux e per quanto possibile su software libero.

Gli studenti possono accedere al chiosco fornendo le credeziali di accesso al SIS (*numero di matricola* e *PIN*), mentre il personale docente e TA fornendo quelle di accesso al sistema di posta elettronica di Ateneo

5 http://www.unipd.it/sis/

6 https://webmail.unipd.it/

7 Nota tecnica: Il servizio si basa sul modulo di autenticazione *pam_http* opportunamente adattato (si veda http://foss.stat.unipd.it/mediawiki/index.php/PAM_http). Il modulo si inserisce nella sequenza di autenticazione standard di un sistema Linux, verificando che le credenziali fornite dall'utente sulla tastiera del chiosco siano valide per l'ingresso in un servizio online predefinito (ad esempio il SIS o la posta elettronica di Ateneo. Se le credenziali risultano valide per il sistema online, pam_http le ritiene valide anche per l'ingresso nel choisco. Altrimenti rifiuta l'ingresso. Il sistema di autenticazione e' completato dal modulo modulo *pam_chuser* (si veda

(*nome.cognome*, *password*). Il controllo sul SIS e' soggetto ad un ulteriore verifica per accertare che possano accedere solo gli studenti muniti di numero di matricola, persone la cui identita' e' stata accertata, e non utenti temporanei (ad es. preiscrizioni). Restano esclusi gli utenti esterni, di tipo c), per i quali la Biblioteca si dovra' fare carico di una completa identificazione, con verifica e registrazione degli estremi del documento. In questo caso si potra' prevedere che l'utente possa accedere *una tantum*, tramite un codice temporaneo che verra' legato alla sua persona e al PC usato solo per il tempo effettivamente passato alla postazione, oppure a credenziali da legare alla persona in modo stabile per un periodo determinato. Per la gestione di questa tipologia di utenti e' in corso di sviluppo un programma apposito, legato a un servizio web. La biblioteca dovra' farsi carico della gestione dei dati personali di utenti esterni, secondo le modalita' prescritte.

Prospettive future:
Nel caso in cui l'impiego di YAK interessi piu' biblioteche, si puo' pensare ad una evoluzione del servizio in cui i dati personali di utenti esterni vengano condivisi tra biblioteche diverse attraverso un archivio centralizzato, in modo che gli utenti identificati e registrati da una biblioteca possano accedere con le stesse credenziali a tutti i terminali YAK.

Caratteristiche tecniche

YAK ha le seguenti caratteristiche tecniche:

- Sistema GNU/Linux basato sulla distribution Debian Sarge
- kernel standard 2.6.8-2 Debian, massima indipendenza dalla piattaforma hardware
- Autenticazione basata su *pam_http* e *pam_chuser*
- Amministrazione remota via *ssh*
- Software installato:
  - Mozilla firefox[a] per la navigazione, completo di plugin flash[b]
  - Terminale x3270[a] per le sessioni OPAC 3270
  - Acrobat Reader 7[b] per leggere i documenti PDF
  - OpenOffice[a] per leggere i documenti della suite MS Office e OpenOffice
  - Ghostview[a]
  - Java virtual machine[b]
- Durata della sessione di lavoro di mezz'ora, passata la quale viene chiusa d'ufficio, configurabile.
- Possibilita' per l'utente di salvare documenti su floppy o dispositivi USB, rilevati automaticamente.
- Supporto Unicode (prinicipali lingue, principali alfabeti).
- Particolare cura della sicurezza e rigorosa limitazione dell'accesso alle risorse locali del PC:

---

http://foss/mediawiki/index.php/Pam_chusur.so) che consente l'apertura di una sessione locale con l'identita' di un singolo utente locale.

a Free software

b Software proprietario gratuito

- nessun account locale oltre a quello amministrativo
- logging remoto
- nessuna interazione col window manager
- nessun desktop manager
- nessuna shell interativa per gli utenti
- resiste agli spegnimenti improvvisi

Problemi aperti:

Opportunita': se le Biblioteche non risultassero soggette alla legge 155/05, verrebbe meno l'esigenza forte di un sistema di autenticazione. Rimarrebbe comunque da adempiere alle esigenze del *linee guida per l'utilizzo delle risorse informatiche*[8] dell'Ateneo, che all'art.23 prescrive che *l'utente esterno* sottoscriva una apposita dichiarazione di responsabilita'.

Appropriatezza: YAK usa per autenticare l'utente delle credenziali che sono state emesse per uno scopo diverso da quello di fornire l'accesso a Internet. Il SIS serve prevalentemente allo svolgimento di pratiche amministrative: pertanto la cura posta dallo studente nel custodire le credenziali potrebbe non essere la stessa richiesta da un sistema di accesso a Internet il cui abuso ha risvolti penali. Non dovrebbero esservi invece problemi legati alla tutela della privacy, in quanto l'accesso a YAK non consente l'accesso a dati che non siano pubblicamente accessibili in Internet. Nel caso della posta elettronica di Ateneo e' gia' richiesto che le credenziali siano custodite con la massima cura, per cui il problema di appropriatezza del loro uso non pare presentarsi.

Tenuta dei log: la normativa prescrive che vengano tenute delle registrazioni del traffico avvenuto dalle postazioni, che pero' non comprendano il contenuto della comunicazione elettronica.

> Decreto del Ministro dell'interno 16 agosto 2005
> *Art. 2. Monitoraggio delle attivita'*
> *1. I soggetti di cui all'art. 1 adottano le misure necessarie a memorizzare e mantenere i dati relativi alla data ed ora della comunicazione e alla tipologia del servizio utilizzato, abbinabili univocamente al terminale utilizzato dall'utente, esclusi comunque i contenuti delle comunicazioni.*

mentre nel caso della comunicazioni telefoniche la terminologia risulta chiara, per comprendere che tipo di registrazione tenere in ambito telematico, e' da chiarire cosa si intenda per *comunicazione* e *tipologia del servizio*.

1. Se per *comunicazione* si intende quella tra PC client (postazione) e server Web, e per *tipologia di servizio* il collegamento al servizio HTTP risiedente sul server, allora bastera' registrare i dati relativi alla sessione IP (indirizzo ip sorgente e destinazione, porta sorgente e destinazione).
   Qualsiasi registrazione relativa a *quale pagina sia stata consultata* andra'

8 http://www.unipd.it/stdoc/lineeguida07092004.pdf

considerato un *contenuto*, e pertanto **non dovra'** essere registrata.

2. Se viceversa si intende, riferendosi all'acceso di servizi WWW, per *comunicazione* quella tra il browser il server Web, allora per *tipologia di servizio* si intendera' l'indirizzo della pagina consultata all'interno dello stesso server web, e quindi andranno registrati anche i dati relativi alla URL consultata.

La prima possibilita' presenta minori difficolta' tecniche: sara' sufficiente installare un programma che tracci il transito dei pacchetti in uscita dalla postazione e non l'attivita' dei programmi. La seconda e' di gran lunga piu' complessa da realizzare, dato che i browser non sono soliti tenere una registrazione delle proprie attivita' e quindi richiederebbe il supporto di un firewall o di un proxy.

Nell'incertezza su quale sia l'interpretazione piu' opportuna del temine *comunicazione*, conviene comportarsi come se fosse valida la prima ipotesi, dato che evita di far registrare dati che che potrebbe *essere vietato* registrare.

Resta comunque aperto il problema non banale di inviare le registrazioni in un archivio centralizzato che le conservi nella modalita' prescritta fino a dicembre 2007 o oltre, se vi fossero proroghe.