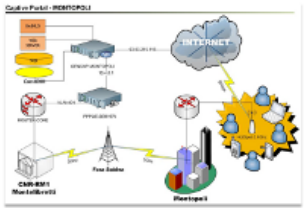
Networking

Un Captive Portal per l'utenticazione su Reti Wifi Dedicate agli Internet Access Point Liberi.†

Augusto Pifferi,*[a] Luca Ianniello,[a] Claudio Ricci,[a] Luigi Rossi,[a] and Marco Simonetti[a]



In questo documento verrà descritta l'attività di realizzazione di un sistema Captive Portal per l'accesso a internet sviluppato dal Servizio Reti dell'Area della Ricerca RM1. Il progetto aveva per obiettivo quello di consentire ai comuni dell'area sabina di offrire ai propri cittadini e visitatori un accesso a internet gratuito e sicuro. Descriveremo le specifiche di progetto, l'architettura, il software e i risultati ottenuti in termini di accessi registrati in un arco di tempo.

Keywords: Captive Portal, Hotspot.

1 Introduzione

I piccoli comuni dell'area Sabina hanno scarse opportunità di collegamenti internet veloci e fruibili da tutti. Il Comune di Montopoli di Sabina si è posto il problema di permettere ai propri cittadini e a coloro che visitano il paese, sia a scopo turistico che a scopo lavorativo, di fornire uno strumento di collegamento ad internet libero sull'esempio di altri Enti Locali in altre aree del territorio Nazionale. In virtù della Convenzione Operativa firmata tra il Comune di Montopoli ed il Dipartimento di Progettazione Molecolare del CNR, l'Amministrazione comunale ha chiesto all'Istituto di Cristallografia di allestire una piattaforma **CAPTIVE PORTAL** per l'autenticazione e registrazione di utenti per il libero accesso alla navigazione internet ed installare un primo wireless Hotspot nella piazza comunale.

Il portale, deve essere in grado di consentire la navigazione internet con procedure semplici di registrazione dell'utente e presentare nella sua pagina iniziale il riferimento al comune quale promotore dell'iniziativa.

2 Il Progetto

La tecnica di Captive Portal forza un client http connesso ad una rete di telecomunicazioni a visitare una speciale pagina web (usualmente per l'autenticazione) prima di poter accedere alla navigazione. Ciò si ottiene intercettando tutti i pacchetti, relativi a indirizzi e porte, fin dal momento in cui l'utente apre il proprio browser e tenta l'accesso a Internet. In quel momento il browser viene rediretto verso una pagina web la quale può richiedere l'autenticazione oppure semplicemente l'accettazione delle condizioni d'uso del servizio o una pagina pubblicitaria.

Il termine Hotspot comunemente si riferisce ad un'intera area dove è possibile accedere ad Internet in modalità senza fili (wireless), attraverso l'uso di un Router collegato a un provider di servizi Internet.

Nell'accezione generica del termine è possibile trovare ormai Hotspot per accedere ad Internet in ristoranti, stazioni ferroviarie, aeroporti, librerie, alberghi, centri commerciali ed in moltissimi altri luoghi aperti al pubblico. Anche diverse amministrazioni locali hanno avviato un piano di accesso pubblico spesso gratuito.

Tuttavia, in Italia si possono individuare ancora pochi punti di accesso realmente gratuiti per accedere alla Rete in questa modalità. Dal punto di vista economico, le tipologie di accesso sono molteplici ma la maggior parte degli esercizi pubblici mette a disposizione il proprio Hotspot dietro pagamento di tariffe a gettone, che dipendono dal tempo di collegamento del client piuttosto che dall'effettivo uso delle risorse di rete.

Per questo motivo, unitamente ad una legislazione particolarmente restrittiva ancora oggi non del tutto superata, in Italia questo tipo di servizio si è diffuso tutto sommato in misura ridotta e solo di recente, rispetto alle medie europee.

3 Specifiche del progetto

Le specifiche richieste per il Captive Portal sono:

- Uso di un software Open Source su piattaforma Linux;
- Pagina di registrazione utenti per l'ottenimento delle credenziali d'accesso;

[a] *CNR - Istituto di Cristallografia, Strada Provinciale 35/d, Montelibretti, Italia*

† Rapporto tecnico IC-RM 2013/11 protocollato in data 19/09/2011 n. IC/1616

- Impedire la navigazione ai client non autenticati;
- Limitazione del traffico dati nella misura di banda utilizzabile, dati trasmessi e tempo di collegamento;
- Impedire l'accesso tramite account già connessi;
- Sistemi di sicurezza per la salvaguardia del sistema operativo e dei dati;
- Log degli accessi;
- Recupero della password persa.

La scelta della piattaforma per il Captive Portal è caduta sul software Open Source "CoovaChilli" le cui caratteristiche principali sono mostrate nella figura qui di seguito:

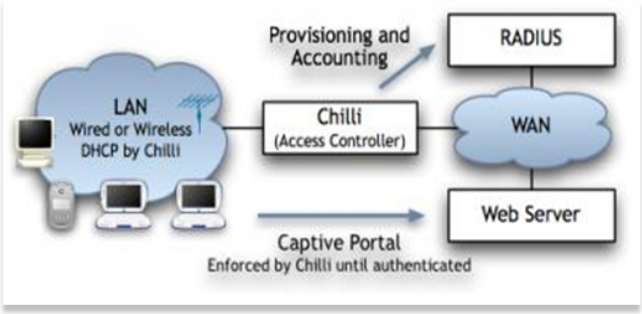


Fig. 1 Schema a blocchi di CoovChili.

CoovaChilli è un Access Control Software che permette la cattura e il reindirizzamento dei pacchetti generati dell'utente che si collega all'HotSpot mostrando una pagina di autenticazione (login) come unica risorsa web consultabile e quindi passaggio obbligatorio per accedere alla navigazione

4 Realizzazione del CAPTIVE

Il Server sul quale è stato installato il Captive Portal ha le seguenti caratteristiche:

Produttore modello	IBM eserver xSeries 345
Processore	Intel(R) Xeon(TM) CPU 3.80GHz L1 cache 8KiB L2 cache 2048KiB Intel(R) Xeon(TM) CPU 3.80GHz L1 cache 8KiB L2 cache 2048KiB
Memoria RAM	Memory 2 GB
Dischi Fissi	SCSI storage PCI-X Fusion-MPT Dual Ultra320 SCSI 36 GB Raid-1 SCSI storage PCI-X Fusion-MPT Dual Ultra320 SCSI 36 GB Raid-1
Scheda video	VGA ATI Technologies Inc. Rage XL

CoovaChilli, il software per il controllo degli accessi, funge da client di un Server RADIUS (**Remote Authentication Dial-In User Service**) che è attualmente lo standard de-facto per l'autenticazione remota tramite un gruppo di protocolli "**AAA**" **Authentication, Authorization e Accounting**, necessari rispettivamente per

Fig. 2 Pagina di reindirizzamento di Coovachili

le funzioni di autenticazione, controllo degli accessi e tracciamento del consumo delle risorse da parte degli utenti.

Uno dei requisiti per il funzionamento dell'applicativo è la presenza del web-server **Haserl** (un programma di 20Kb molto utilizzato nelle apparecchiature embedded) che oltre ad avere come caratteristica principale quella di fungere da demone-web ha anche quella di interpretare bash-scripting (Unix-command-line) per la generazione di pagine dinamiche come un vero e proprio CGI. il Sistema Operativo utilizzato è **GENTOO LINUX** sul quale è stata installata e configurata l'intera piattaforma. Gentoo Linux è una speciale distribuzione di Linux che può essere facilmente ottimizzata e personalizzata per qualsiasi applicazione o necessità. L'estrema velocità, la grande configurabilità e l'ottima collaborazione fra gli sviluppatori e gli utenti sono i grandi punti di forza di Gentoo. Il Server RADIUS utilizzato in questa piattaforma è anch'esso di origine Open Source ed è **FreeRadius**.

Per la parte dei dati relativi alle credenziali d'accesso e gli attributi richiesti per il funzionamento del protocollo "**AAA**", **FreeRadius** e' stato configurato per essere interfacciato con il demone **Mysql**.

Attraverso la pagina di login l'Access Controller instaura la comunicazione con il Server RADIUS il quale a sua volta, seguendo le impostazioni configurate, interroga il data-base per l'avvio dei meccanismi di autenticazione remota (verifica della password, assegnazione di un id univoco, assegnazione attributi di controllo etc.).

Per poter accedere alla navigazione è necessario essere in possesso delle credenziali: una userid e una password.

Poiché il software a disposizione per la gestione delle credenziali d'accesso offre solo un backend da operatori, si è reso necessario studiare e sviluppare un software per la registrazione degli utenti.

Per rendere questo software usufruibile dal più ampio numero di utenti e compatibile con il più ampio numero di dispositivi si è optato per l'utilizzo del linguaggio **PHP** e **JavaScript**.

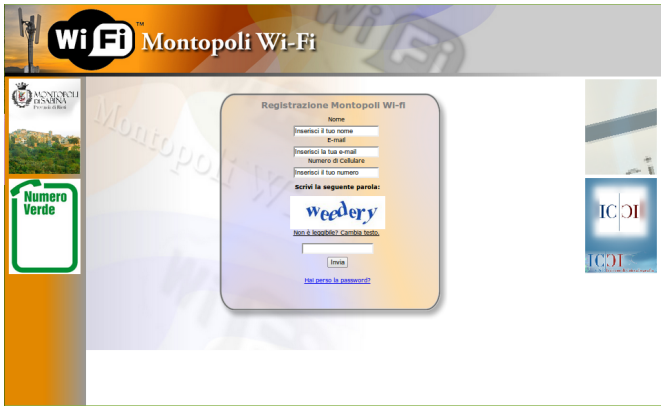


Fig. 3 Pagina di registrazione Captive Montopoli.

L'interfaccia di registrazione (Fig. 3) presenta 4 campi che l'utente che esegue la registrazione è obbligato a riempire:

Il campo Nome, il campo e-mail, il campo numero di cellulare e il campo captcha.

In tutti i campi sono stati impostati dei controlli, a livello software, che obbligano l'utente a compilare i dati richiesti.

Il campo nome non può essere vuoto, deve essere modificato dallo stato di partenza, non deve essere già presente nel DB.

Il campo e-mail non può essere vuoto, deve essere modificato dallo stato di partenza, deve contenere il carattere chiocciola (@) e la parte relativa al dominio deve essere di almeno 5 caratteri compreso punto di separazione.

Il campo numero di cellulare non può essere vuoto e deve contenere solo caratteri numerici e non deve essere già presente nel DB.

In fine il campo **CAPTCHA*** deve essere compilato correttamente per poter superare la verifica. Una volta compilati correttamente tutti i campi richiesti viene spedito un messaggio **SMS** al numero indicato nel form tramite un Gateway GSM; il messaggio contiene la password necessaria all'accesso. Questo meccanismo fa si che l'utente che compila il campo numero di cellulare con dati mendaci non sarà poi abile ad effettuare l'accesso alla navigazione in quanto non provvisto della necessaria password.

E' stato previsto e sviluppato anche il software per il recupero della password per tutti quegli utenti che hanno già effettuato la registrazione ma non sono più in possesso del messaggio SMS originale contenente la

Fig. 4 Frame della registrazione utente

Fig. 5 Frame per il recupero password.

* Con l'acronimo inglese CAPTCHA si denota nell'ambito dell'informatica un test fatto di una o più domande e risposte per determinare se l'utente sia un umano (e non un computer o, più precisamente, un bot). L'acronimo deriva dall'inglese "Completely Automated Public Turing test to tell Computers and Humans Apart" (Test di Turing pubblico e completamente automatico per distinguere computer e umani)

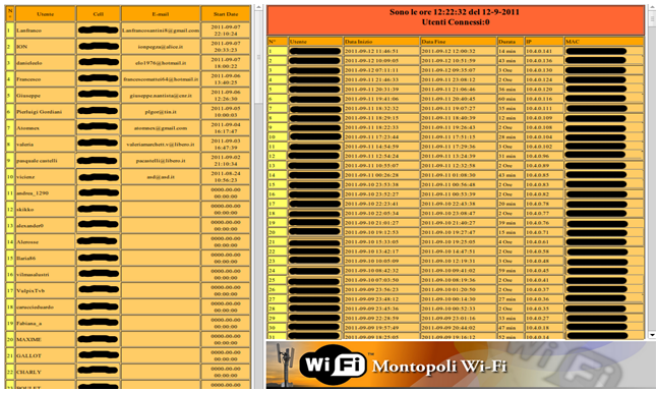


Fig. 6 Registrazione degli accessi al Captive Portal.

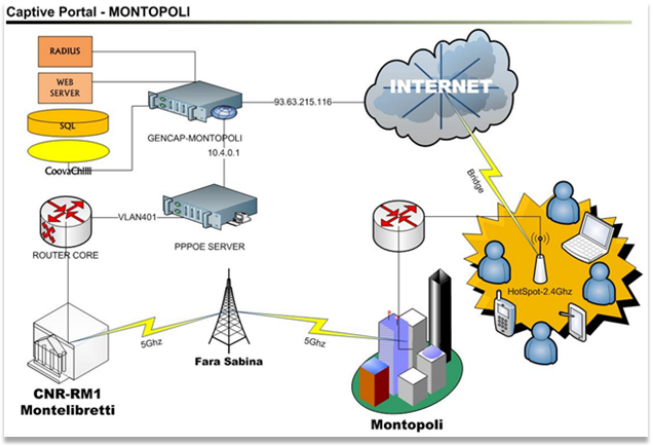


Fig. 7 Layout di funzionamento della “Piazza digitale” realizzata a Montopoli di Sabina

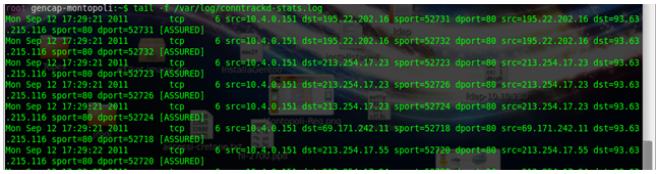


Fig. 8 Schermata del demone Conntrackd che mostra le connessioni stabilite con successo.

password.

Utilizzando l’apposito link, presente sia nella pagina di registrazione ”*Hai perso la password?*” che nella pagina di login “*Password dimenticata? Clikka qui*!” è possibile recuperare la propria password di accesso inserendo il numero di telefono utilizzato durante la registrazione nell’apposito campo del form insieme al codice CAPTCHA corretto, in questo modo si invia una richiesta al server dati (MySQL) che, una volta trovata corrispondenza tra gli utenti registrati, spedisce tramite un messaggio SMS la password al numero di telefono in questione.

Per tenere sotto controllo il flusso di accessi ma soprattutto per capire meglio l’ottica e la portata dell’impatto del progetto stesso è stata sviluppata anche una pagina WEB che riporta in real-time gli accessi e le registrazioni che vengono effettuate tramite il portale (Fig. 6).

Nella colonna a sinistra della pagina sono elencati i dati inseriti al momento della registrazione: nome, numero di cellulare, e-mail e data registrazione.

Nella colonna a destra sono mostrati: l’utente identificato dal numero di telefono, la data e l’ora di inizio e fine collegamento dal momento dell’avvenuto login con successo, la durata effettiva della connessione, il MAC-ADDRESS e l’indirizzo IP associato.

In 5 mesi di funzionamento dell’HotSpot risultano effettuate 97 registrazioni e 1660 accessi.

5 L’Access Point di Montopoli di Sabina (RI)

Nella Piazza Comunale a Montopoli di Sabina è stato installato un Router con una interfaccia LAN Wireless 2.4Ghz che funge da punto di accesso per l’HotSpot.

Lo stesso router ha una interfaccia WAN 5Ghz che viene usata per effettuare la connessione alla rete Wireless verso il CNR passando attraverso la dorsale che si appoggia a Fara Sabina.

La connessione viene garantita, autenticata e autorizzata tramite un link PPPoE verso l’apposito server PPPoE in sede CNR (che è direttamente interfacciato a un server RADIUS per svolgere le idonee operazioni AAA).

Appena in rete il router di Montopoli instaura una comunicazione (questa volta PPTP) con un router di core, anch’esso posizionato nei CED dell’Area della Ricerca RM 1.

L’ultima operazione che viene compiuta da questi sistemi è la realizzazione di un bridge fra la LAN 2.4Ghz di Montopoli e la VLAN in cui risiede il captive portal. In questo modo chi si collega alla rete wireless di Montopoli si trova nello stesso dominio di broadcast del captive portal, ottiene dinamicamente un indirizzo IP e viene intercettato dal sistema che richiede la fase di autorizzazione/autenticazione prima di concedere l’accesso a internet.

La particolare struttura del Portale fa si che tutti gli utenti che ottengono l’accesso alla navigazione vengano identificati su internet attraverso lo stesso indirizzo IP pubblico a causa del mascheramento che viene effettuato da parte del gateway, in questo caso CoovaChilli, per il transito dei pacchetti.

Per garantire comunque la rintracciabilità dell’utilizzatore finale, nel caso di eventuali infrazioni delle normative vigenti, e stato installato e configurato un software, sempre di matrice Open Source, dal nome Conntrackd.

Questo demone si occupa di registrare L’indirizzo IP sorgente e quello di destinazione di tutte le connessioni che avvengono attraverso il Captive Portal.

Per evitare di registrare informazioni non pertinenti ed inutili, il demone è stato configurato in modo da tenere traccia solo dei collegamenti che vanno a buon termine

quindi che arrivano allo stato di **ESTABILISHED** o come riporta il demone stesso **ASSURED**.

Registrando solo e unicamente gli indirizzi IP (sorgente e destinazione) si garantisce agli utilizzatori finali l'anonimato della navigazione e quindi il rispetto della privacy poiché con i dati registrati e' possibile risalire solo ai server contattati e non alle pagine visualizzate.

Per quanto riguarda la navigazione agli utenti e' stato concessa piena liberta di utilizzo limitando, tramite RADIUS, l'accesso simultaneo da parte di più utenti con le stesse credenziali e permettendo un limite massimo di traffico dati al giorno di 500MB.

6 Conclusioni

Rispetto ad altri paesi, in Italia solo ora si stanno attuando politiche di accesso libero ad internet conformando la nostra legislazione, il più delle volte molto restrittiva, a quella più liberale della Comunità Europea e dell'area Americana. Il disagio derivante dalla difficoltà di collegamento ad internet dei giovani, soprattutto nelle realtà dei piccoli comuni e nelle aree rurali, è ancora fortemente sentito. Molti Enti Locali, Province e Regioni si stanno muovendo in questa direzione promuovendo progetti per l'attivazione di quanti più Access Point liberi possibile sul territorio (ad esempio "Provincia WiFi" della Provincia di Roma con la quale l'istituto di Cristallografia collabora ormai da più di due anni). Nella provincia di Rieti questa è la prima collaborazione tra Consiglio Nazionale delle Ricerche ed Enti Locali per la realizzazione di "Piazze digitali" che si è subito rivelato un successo.

Sull'onda di questo risultato si sono rivolti al nostro Istituto WISP (Wireless Internet Service Provider) locali per la realizzazione di impianti simili presso esercizi pubblici privati (Acquapiper di Guidonia e Terme di Cretone) concretizzando una reale collaborazione fra Enti di Ricerca e privati.

Riferimenti

1 A. Pifferi, G. Agostini, M. Catricalà, A. D. Simone, L. Ianniello, G. Nantista, C. Ricci, L. Rossi, M. Simonetti, (PM.P07.014.005) Sviluppo ed applicazioni di reti telematiche anti "Digital Divide": LA STAZIONE DI TRASMISSIONE WIRELESS NEL COMUNE DI MONTOPOLI DI SABINA".Istituto di Cristallografia-Rapporto Tecnico IC-RM 11/07 prot. 1500 del 05/08/2011.

2 http://www.coova.org/.

3 http://www.gentoo.org/.

4 http://freeradius.org/.

5 http://conntrack-tools.netfilter.org/.