Il progetto INFN TRIP e EduRoam

Alessandro Brunengo[1], Roberto Cecchini[2], Luca dell'Agnello[3] Mirko Corosu[1], Enrico M. V. Fasanelli[4], Ombretta Pinazza[5], Riccardo Veraldi[2]

Abstract

Viene descritto il progetto di AAI realizzato in ambito INFN.
Il progetto ha utilizzato i risultati di EduRoam, combinando i metodi di autenticazione via 802.1x e via web portal. L'autenticazione è trasparente per l'utente, se dotato di un certificato X.509. Il meccanismo è compatibile con quello utilizzato da EduRoam (proxying di server RADIUS).

Introduzione

Il progetto TRIP (The Roaming INFN Physicist) è nato circa due anni fa in ambito INFN con lo scopo di ridurre i problemi che gli utenti roaming devono affrontare. In particolare:

- l'utilizzo da remoto dei servizi della Struttura di appartenenza;
- l'utilizzo dei servizi della Struttura ospitante (ad es. le stampanti).

Questo richiede opportune configurazioni, non solamente dei server remoti, ma anche di quelli della rete locale cui ci si sta collegando: ad esempio è necessario che il system manager locale abiliti il server dhcp a rilasciare un indirizzo ip al portatile del viaggiatore.

Il supplemento di autenticazione e autorizzazione necessario si traduce in un aggravio di lavoro per il system manager e inconvenienti per il viaggiatore.

Una volta risolto il problema della concessione all'ospite dei permessi necessari per accedere alle risorse della sua Struttura di appartenenza (in pratica l'assegnazione di un indirizzo IP), si presenta quello ben più difficoltoso dell'accesso ai servizi della Struttura ospitante. In questo caso è necessario che le informazioni di autorizzazione vengano trasmesse dalla Struttura di appartenenza a quella ospitante, non essendo pensabile la loro duplicazione. In altri termini è necessaria la realizzazione di un meccanismo di *Authentication and Authorization Infrastructure* (AAI), che può essere schematizzato nei punti seguenti:

- autenticazione dell'utente a cura della Struttura ospitante;
- richieste dell'utente;
- trasmissione delle richieste alla Struttura di appartenenza per verificarne la legittimità;
- trasmissione dell'autorizzazione dalla Struttura di appartenenza a quella ospitante.

Siamo partiti dai risultati della Task Force di TERENA sulla mobility [TFM] e, ovviamente nel rispetto delle nostre necessità, abbiamo cercato soluzioni compatibili con un'analoga iniziativa, che coinvolge molte reti di ricerca europee (EduRoam [EDU]).

[1] INFN, Genova.
[2] INFN, Firenze.
[3] INFN, CNAF.
[4] INFN, Lecce.
[5] INFN, Bologna.

Il progetto

I meccanismi che sono stati presi in considerazione, anche alla luce delle esperienze altrui, e il fatto che per i nostri scopi era essenziale avere autenticazioni **multipiattaforma** basate sia su X.509 sia su sistemi di autenticazione locale (ad es. Kerberos e LDAP) sono i seguenti:

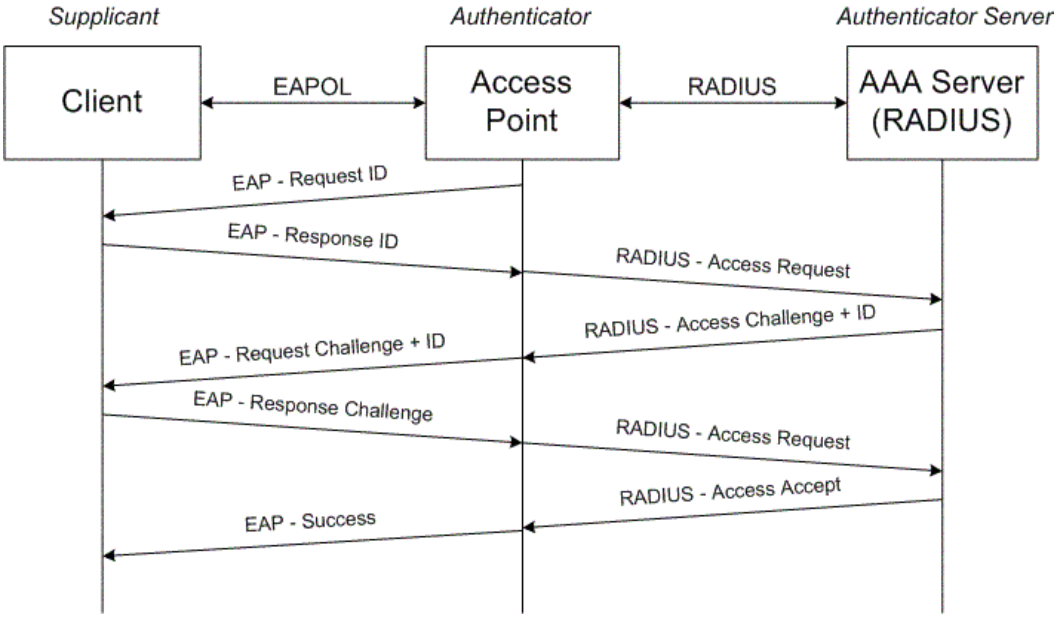
- 802.1X;
- web portal:
- VPN (non approfondito nel corso del progetto per mancanza di risorse).

In tutti i casi il server di autorizzazione è un server **Radius**, attualmente lo standard di fatto nel settore.

802.1x

Supporta numerosi metodi di autenticazione, in particolare via certificato X.509, particolarmente interessante vista l'esistenza di una Certification Authority per l'INFN (INFN CA), in funzione ormai da diversi anni e il fatto che l'uso dei certificati è molto diffuso in ambito INFN, grazie anche all'impegno dell'ente nei progetti GRID.

Il complesso delle comunicazioni fra supplicante, access point e server di autenticazione è schematizzato nella figura seguente:



Web Portal

Consente l'autenticazione con username / password o certificato X.509 (via Apache SSL).

L'utente, prima di poter accedere alla rete, si deve autenticare tramite una pagina web: l'autenticazione è trasparente se si possiede un certificato X.509 riconosciuto dal server.

In particolare, il client, dopo che si è collegato all'Access Point, ottiene un indirizzo IP dal DHCP server della VLAN ospiti. Questo indirizzo è bloccato da un Gateway, che intercetta il traffico HTTP e lo dirotta verso il server RADIUS di autenticazione. Ad autenticazione effettuata, il Gateway permette il passaggio del traffico.

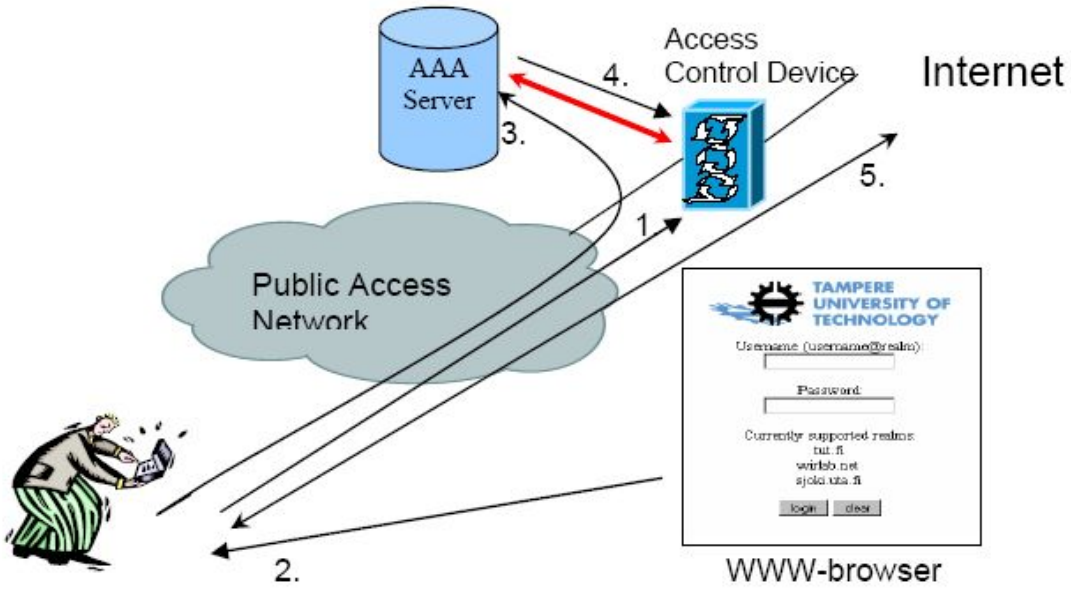


Figure 1. Web portal (da [TFM])

Una soluzione, basata su **FreeRadius** [FRA] e il portale **NoCat** [NOC], è in uso presso la Sezione di Genova [TRG].

Un'altra soluzione, basata su **FreeRadius** e il portale **tino** [TIN], è in uso presso la Sezione di Firenze.

Proxying

Il server RADIUS può essere utilizzato anche in modalità *proxy*, in modo da consentire all'utente remoto di autenticarsi con il server del proprio istituto. In questo caso è importante che siano ben chiari i problemi di scurezza legati al meccanismo di autenticazione.

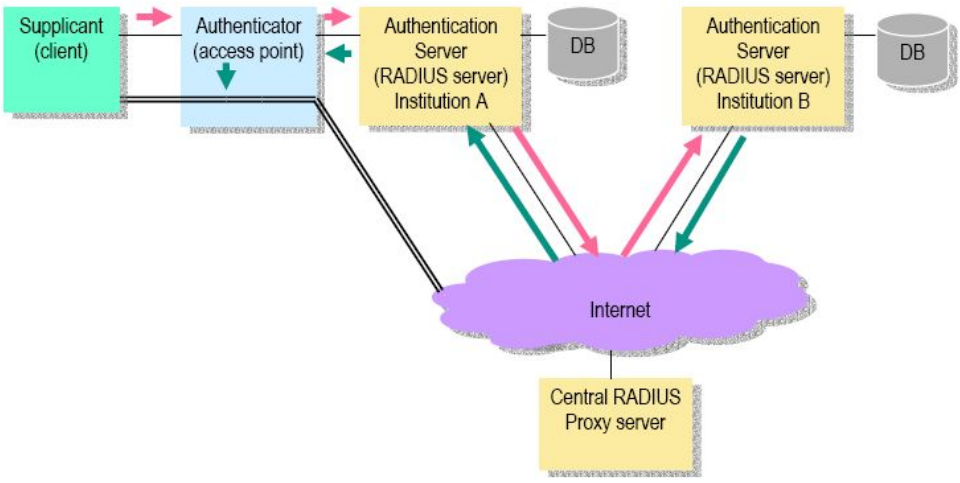


Figure 2. Autenticazione via proxying (da [TFM])

Questo è il meccanismo in uso nel progetto EduRoam [EDU]. Presso la Sezione INFN di Firenze

è stato installato il server RADIUS nazionale, collegato a quello di top level europeo.

Conclusioni

Allo stato attuale la migliore soluzione sembra quella di utilizzare sia l'802.1x sia un Web Portal. Alcuni Access Point sono in grado di gestire entrambi i metodi contemporaneamente (su SSID diversi) .

Gli utenti muniti di un certificato X.509 valido (e della giusta combinazione di hardware e software) possono utilizzare l'autenticazione trasparente via 802.1x. Gli altri dovranno passare dal Web Portal.

Rimangono da chiarire i problemi di sicurezza legati al meccanismo di autenticazione via proxy, utilizzato da EduRoam.

I futuri sviluppi prevedono l'utilizzo di sistemi one-time password, l'utilizzo di smartcard usb e l'integrazione con Kerberos.

Maggiori informazioni sullo stato del progetto sono disponibili su [ITR].

Bibliografia

[EDU]
http://www.eduroam.org/

[FRA]
http://www.freeradius.org/

[ITR]
http://security.fi.infn.it/TRIP/

[NOC]
http://nocat.net/

[TIN]
http://www.cc.puv.ti/~teu/tino/

[TFM]
TERENA Mobility Task Force, http://www.terena.nl/tech/task-forces/tf-mobility/

[TRG]
http://trip.ge.infn.it/

Biografie degli autori

Alessandro Brunengo

Laureato in Fisica nel 1991, è responsabile del Servizio Calcolo della sezione INFN di Genova dal 2001. Dal 2001 è rappresentante della sezione in seno alla Commissione Calcolo e Reti INFN.

Roberto Cecchini

Laureato in Fisica, è responsabile del Servizio Calcolo e Reti della Sezione INFN di Firenze, dal 1999 è responsabile del servizio di sicurezza informatica della rete GARR (GARR-CERT), dal 1998 gestisce la Certification Authority dell'INFN (INFN CA).

Mirko Corosu

Laureato in Fisica nel 1999, è membro del Servizio Calcolo della sezione INFN di Genova dal 2003. Si è occupato della configurazione e installazione di servizi centrali e di farm per calcolo scientifico.

Luca dell'Agnello

Laureato in Fisica nel 1992, è responsabile delle operations del Tier1 INFN dal 2004. Si occupa di sicurezza, avendo partecipato, nell'ambito dei progetti europei Datagrid e Datatag, alla progettazione e sviluppo del VOMS.

Enrico M. V. Fasanelli

Laureato in Fisica nel 1991, è responsabile del Servizio di Calcolo e Reti della sezione INFN di Lecce dal 1996. Dal 1999 è il rappresentante della Sezione in seno alla Commissione Calcolo e Reti dell'INFN.

Ombretta Pinazza

Laureata in Fisica nel 1996. Lavora nel Servizio Calcolo e Reti della Sezione INFN di Bologna dal 1998. Lavora anche nel monitorong online per l'esperimento ALICE.

Riccardo Veraldi

Laureato in Fisica nel 1997. Lavora nel Servizio Calcolo e Reti della Sezione INFN di Firenze dal 2000. Si occupa di problemi legati alla sicurezza dal 1997.