Infrastruttura di accesso alla rete Unimib

Autori: Stefano Moroni – Università di Milano Bicocca

Abstract
Scopo del presente lavoro è offrire un esempio di implementazione reale di infrastrutture di AAA e PKI per l'accesso e la mobilità in contesti di grandi dimensioni ad alta disponibilità (HA) e multi-vendor. L'intero progetto è basato su software non-proprietari (open source) e protocolli standard (suite TCP/IP e relativi Internet Standard IETF e 802 IEEE Working Group).

Vengono descritte le strategie seguite e le scelte adottate nella realizzazione dell'infrastruttura di accesso alla rete di campus IP/MPLS dell'Università di Milano Bicocca.
Per infrastruttura di accesso si intende quella parte di funzionalità di una rete preposta alla gestione delle varie modalità di connessione e che implementa l'insieme di regole e politiche relative alle diverse tipologie di utenza. La definizione dei requisiti di tale infrastruttura è guidata dalla necessità di garantire accesso a rete e servizi di rete all'intera comunità universitaria, inclusi studenti e ospiti, con la massima semplicità possibile compatibilmente a un adeguato livello di sicurezza.

Scenario
La rete di campus univesitaria comprende oltre 20.000 punti di rete, 15.000 porte sugli apparati del livello di accesso, 13.000 terminali connessi permanentemente in rete cablata e la copertura wireless completa degli edifici del campus per un totale di 250.000 mq. Il bacino di utenza, offrendo connettività e servizi agli studenti, è di oltre 40.000 unità. Questi numeri rendono indispensabile una infrastruttura di accesso affidabile e scalabile.

Definizione dei vincoli e degli obiettivi del progetto
In funzione dell'utilizzo dei luoghi, della categoria di utenza e della mobilità richiesta è necessario fornire il tipo di connettività adeguato, il relativo livello di riservatezza, sicurezza e l'eventuale necessità di autenticazione.
Le stesse tecnologie di connettività utilizzate (es. wired or wireless) richiedono differenti livelli nell'implementazione delle tecniche di protezione del canale di accesso.
La logica della gestione di queste esigenze nel tipo di accesso deve essere il più possibile trasparente all'utente e di facile amministrazione da parte del personale addetto al controllo e monitoraggio della rete. Allo stesso modo devono essere in grado di ottenere l'accesso alla rete tutti i principali sistemi operativi e le loro implementazioni hardware.
Le credenziali degli utenti devono essere uniche sia per l'accesso alla rete che per l'accesso a tutti I servizi universitari. Questo vincolo porta alla necessità di utilizzare un meccanismo di autenticazione resistente a eavesdropping in quanto

l'integrità di tali credenziali, il cui possesso dà accesso a tutti i servizi dell'Università e ai dati riservati degli utenti, deve essere garantita.

Implementazione.
Nel caso dei terminali fissi connessi in rete di docenti e personale strutturato, non essendoci esigenza di mobilità ed essendo noti gli utenti, si assegna un indirizzo IP statico registrato nel DNS di ateneo e si richiede solo autenticazione in locale alla macchina.
Nelle aree comuni (aule, sale riunioni, zone studio...) l'identità degli utenti che richiedono accesso alla rete non è nota a priori ed è necessario un meccanismo per il riconoscimento e le autorizzazioni dei medesimi.
Per l'autenticazione in rete dei terminali mobili si sceglie il framework 802.1X con EAP-TLS e mutua autenticazione tra supplicant e authentication server con certificati X.509; nel caso 802.11i (wireless) si implementa AES per il tratto on air. L'assegnazione dell'indirizzo IP avviene tramite protocollo DHCP con relay agent sui nodi di accesso al backbone.

La discriminazione del tipo di utenza mobile che si connette alla rete e l'assegnazione delle autorizzazioni relative alla categoria di appartenenza è operata tramite una infrastruttura di Autenticazione, Autorizzazione e di Accounting (AAA) realizzata su protocollo Radius, con un directory server LDAP, per le credenziali utente, e una infrastruttura a
chiave pubblica (PKI) per la generazione dei certificati personali X.509 degli utenti.
Per ogni profilo di utenza si definisce un REALM: name.surname@unimib.it, name.surname@campus.unimib.it, name.surname@guest.unimib.it.
La registrazione degli utenti nel directory server centrale avviene all'atto della immatricolazione, per gli studenti, o della presa di servizio, per docenti, personale strutturato e collaboratori.
Per la generazione dei certificati utente è stata sviluppata una procedura on-line il cui front end è raggiungibile su protocollo https e che utilizza per l'autenticazione degli utenti il servizio di directory centralizzato LDAP. Una volta autenticato, l'utente inserisce i dati richiesti per la produzione del certificato (firmato dalla CA di ateneo) e opera il download della coppia certificato/chiave privata. Per convegni e ospiti occasionali la generazione dei certificati X.509, a durata limitata, avviene tramite la stessa procedura on-line da parte di personale autorizzato.

Nell'architettura di AA i diritti e i permessi relativi alle categorie di utenza, e che quindi ne determinano le Autorizzazioni, vengono implementati tramite la definizione di gruppi LDAP ai quali gli utenti vengono associati tramite il proprio "dn" (distinguished name).
All'interno del gruppo di autorizzazione, il server RADIUS opera una ulteriore differenziazioni dei privilegi in funzione del REALM dell'utente. Per gli utenti Eduroam, cioè per quelli il cui REALM non appartiene al dominio unimib.it, l'autenticazione viene proxata al Radius server di appartenenza.

Al termine del processo di autorizzazione i diritti dell'utente determinano l'inserimento in vlan 802.1Q sugli apparati di accesso e l'assegnazione a classi di servizio sul backbone IP/MPLS della rete.
Con la connessione inizia la fase di accounting radius. I dati di accounting vengono incrociati con le tabelle DHCP per ottenere l'associazione username/IP address e vengono inseriti in un database relazionale dove vengono conservati per un periodo conforme alle normative di legge in materia.
Per il controllo degli accessi e il monitoraggio delle connessioni si è sviluppato un applicativo basato su SNMP che fornisce i parametri delle connessioni in tempo reale.
Dopo più di un anno di progettazione e di test bed l'infrastruttura è entrata in produzione nel 2007.

Problematiche e difficoltà affrontate.
La complessità del progetto risiede nel fatto che si è dovuto realizzare il tessuto connettivo tra le sue parti funzionali che operano ai livelli 2, 3 e 4 del modello di riferimento ISO/OSI, e tra queste e lo strato di AAA.
Nella sua realizzazione i problemi maggiori sono stati riscontrati nella non sempre corretta implementazione degli standard di rete da parte dei produttori di apparati di rete testati Va però detto che con questi si È instaurata una profiqua collaborazione per la correzione delle varie release di firmware.
Per la realizzazione della parte di controllo e monitoraggio degli accessi 802.1X si sono dovute utilizzare anche le estensioni MIB vendor specific (estensioni proprietarie del MIB tree).
Gli apparati di accesso layer2 (802.1X enabled) nella loro funzione di authenticator 802.1X non sempre implementano tutti gli attributi di radius accounting necessari alla definizione delle connessioni.
Nella realizzazione dell'archivio delle connessioni, per ottenere l'associazione username-leased IP address, si devono incrociare i dati del sever DHCP con quelli del processo 802.1X (l'authenticator 802.1X opera a livello 2 e l'assegnazione dell'indirizzo di livello 3 al supplicant è posteriore); una implementazione non rigorosa degli standard utilizzati o un suo difetto in una qualunque parte avrebbe conseguenze sull'intero processo.
La scelta di EAP-TLS, comportando l'utilizzo di una PKI, implicava la verifica dell'affidabilità dei supplicant installati sulle piattaforme portatili per la gestione delle chiavi crittografiche (l'implementazione diffusa di tale tecnologia è relativamente recente). Inoltre non era facile stimare l'impatto dell'uso dei certificati sull'utenza; il rischio era di scoraggiare l'utenza meno esperta. La realizzazione della procedura on line per la generazione e la distribuzione dei certificati e la sensibilizzazione dell'utenza sul problema rappresentato dalla sicurezza ha avuto il successo sperato e i numeri (oltre 8.000 certificati validi emessi di cui circa 6.000 agli studenti) confermano la bontà della strada intrapresa. È stato anche realizzato un portale web informativo ad accesso libero dedicato alle informazioni sulla procedura di accesso e contenente la configurazione guidata per I principali sistemi operativi. Il fatto che, una volta installato il certificato sul terminale utente, l'accesso alla rete avviene

automaticamente è stato il fattore determinante per la diffusione dell'utilizzo tra gli utenti.
Per l'infrastruttura a chiave pubblica si è dovuto sospendere l'utilizzo del progetto OpenCA in quanto ancora acerbo e non scalabile a grandi numeri. Nella realizzazione della procedura on line per la generazione d il download dei certificati X.509 degli utenti questo ha comportato un lavoro extra per l'interfacciamento dell'application server alle API di una CA proprietaria.
I software open-source utilizzati (OpenLDAP, FreeRADIUS, MySQL) si sono dimostrati assolutamente stabili e non hanno comportato difficoltÃ nell'implementazione in ambienti clusterizzati e in HA.