Mobile Authentication

Nomadi VS o-admin

Enrico M. V. Fasanelli INFN Sezione di Lecce

SOMMARIO

- “Cenni storici”
- Tutto quello che l’utente mobile vorrebbe avere (e che purtroppo ha già iniziato a chiedere)
- Il punto di vista dell’amministratore
- Le possibili soluzioni
- Il progetto TRIP
- Lo stato di avanzamento dei lavori

La storia

- Presentazione di “Perini” a WSCR2003 @Paestum: **La Posta !**
  - CRITICO
    - ottenere un indirizzo IP registrato nel DNS (alcuni siti non accettano connessioni da IP non registrati)
  - RILEVANTE
    - poter usare il mail server (magari senza cambiare la configurazione del proprio MUA)
  - DESIDERABILE
    - avere un dial-in accessibile in ogni sezione (per lavorare dall’albergo?)
    - potersi collegare alla LAN dell’istituto ospitante (dopo eventuale registrazione)

L'utente girovago (come me)

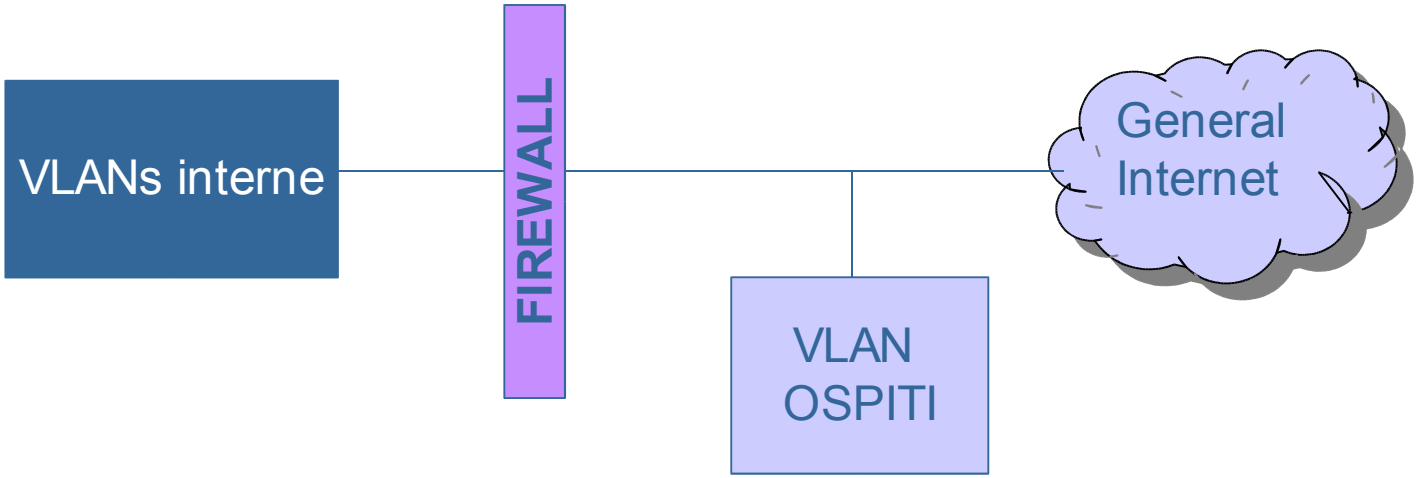
- L'utente girovago vuole poter accedere ai servizi di rete nella sede ospitante
  - Indirizzo IP "vero"
    - NAT può causare problemi con ad es. AFS o con alcuni VPN box (precedenti al NAT-T)
  - Accesso ad un server SMTP ed al prorpio server IMAP
    - SMTP server abituale, magari con autenticazione via TLS (o anche via VPN sulla propria LAN)
    - SMTP server locale in mancanza di autenticazione presso il server abituale o in presenza di filtri su SMTP/VPN della LAN ospitante
  - Accesso al sistema di stampa locale
  - Accesso a file sharing delle LAN di origine ed ospitante
    - VPN libero
    - File sharing anche fuori da eventuale dominio AD

Il [sys|net|sec]-admin (come me)

- vuole
  - far funzionare la rete ed i servizi
  - permettere che gli ospiti possano collegarsi ed usufruire dei servizi
  - usare quanto più possibile servizi ed infrastruttura esistente per i propri utenti
- NON vuole
  - i barbari dentro le mura
  - gestire database ad hoc per gli ospiti

Come fare?

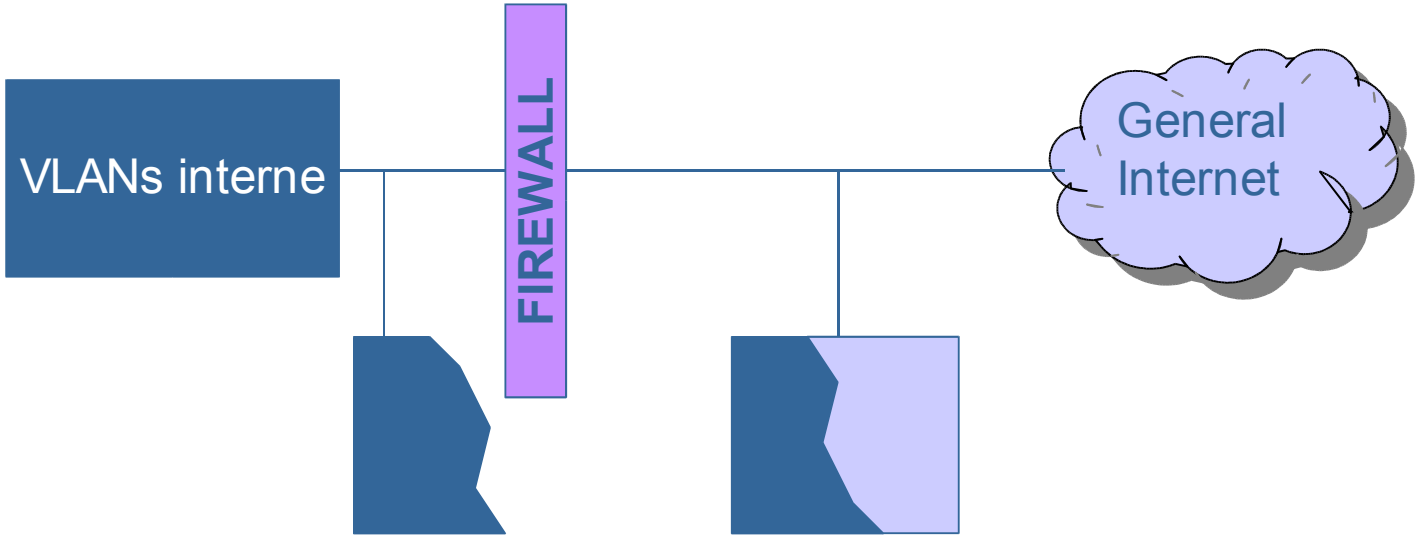
- Tengo i barbari fuori dalle mura
- Non gestisco database ad hoc



- pro
  - garantisce VPN, SMTP, WEB
- contro
  - impedisce accesso ai servizi della LAN
  - permette l'accesso a chiunque

Autenticabilità

- Ci sono ospiti che sono “più ospiti di altri” che, se autenticati, potrebbero accedere alla LAN interna.



Con quali strumenti?

- VPN
  - funziona a L3, richiede un client ad hoc, fa riferimento (e permette il collegamento) alla LAN remota
- Portale WWW
  - funziona a L3 e quindi l'ospite deve avere un indirizzo IP (anche se in rete privata) ed accesso alla LAN
- 802.1X
  - Ve ne parla Ombretta Pinazza

TRIP
(The Roaming INFN Physicist)

Commissione Calcolo & Reti
Roma 7-9 ottobre 2003

Enrico M. V. Fasanelli INFN Sezione di Lecce

Il progetto originale (in parole)

Quello che ci proponiamo di realizzare è un'architettura hw e software che permetta la facile autenticazione e autorizzazione del viaggiatore, senza che questo debba preventivamente comunicare la sua presenza al system manager locale. Ad autorizzazione avvenuta il viaggiatore sarà in grado di accedere ai servizi della rete che il responsabile locale avrà autorizzato: tipicamente ottenere un indirizzo IP per raggiungere la propria sede remota, ed avere accesso ai servizi essenziali forniti dalla sede locale (Printing, relay SMTP, file sharing, ecc. ecc.).

Un beneficio aggiuntivo sarà un miglioramento della sicurezza della rete, wireless in particolare, visto che l'accesso sarà basato su controlli più sicuri di quelli sulla semplice esistenza di un mac address in un database di autorizzazione

I meccanismi che intendiamo prendere in considerazione, anche alla luce delle esperienze altrui, sono i seguenti

- 802.1X,
- "web based"

In entrambi casi il server di autorizzazione sarà un server Radius, che è attualmente lo standard di fatto nel settore

Il progetto originale (in cifre)

- 12 mesi di durata
- 6 mesi per il primo deliverable
  - testbed per dimostrare la funzionalità
- 9 persone
  - Cecchini (promotore e responsabile nazionale), Dell'Agnello, Fasanelli, Pinazza, Veraldi
  - + Brunengo, Corosu, Giacomini, Mazzoni
- 6 sedi
  - CNAF, Bologna, Firenze, Lecce
  - + Genova, Pisa
- meccanismi da valutare
  - 802.1X, web-based
  - +VPN
- 1 AAI *(Authentication and Authorization Infrastructure)*
  - RADIUS

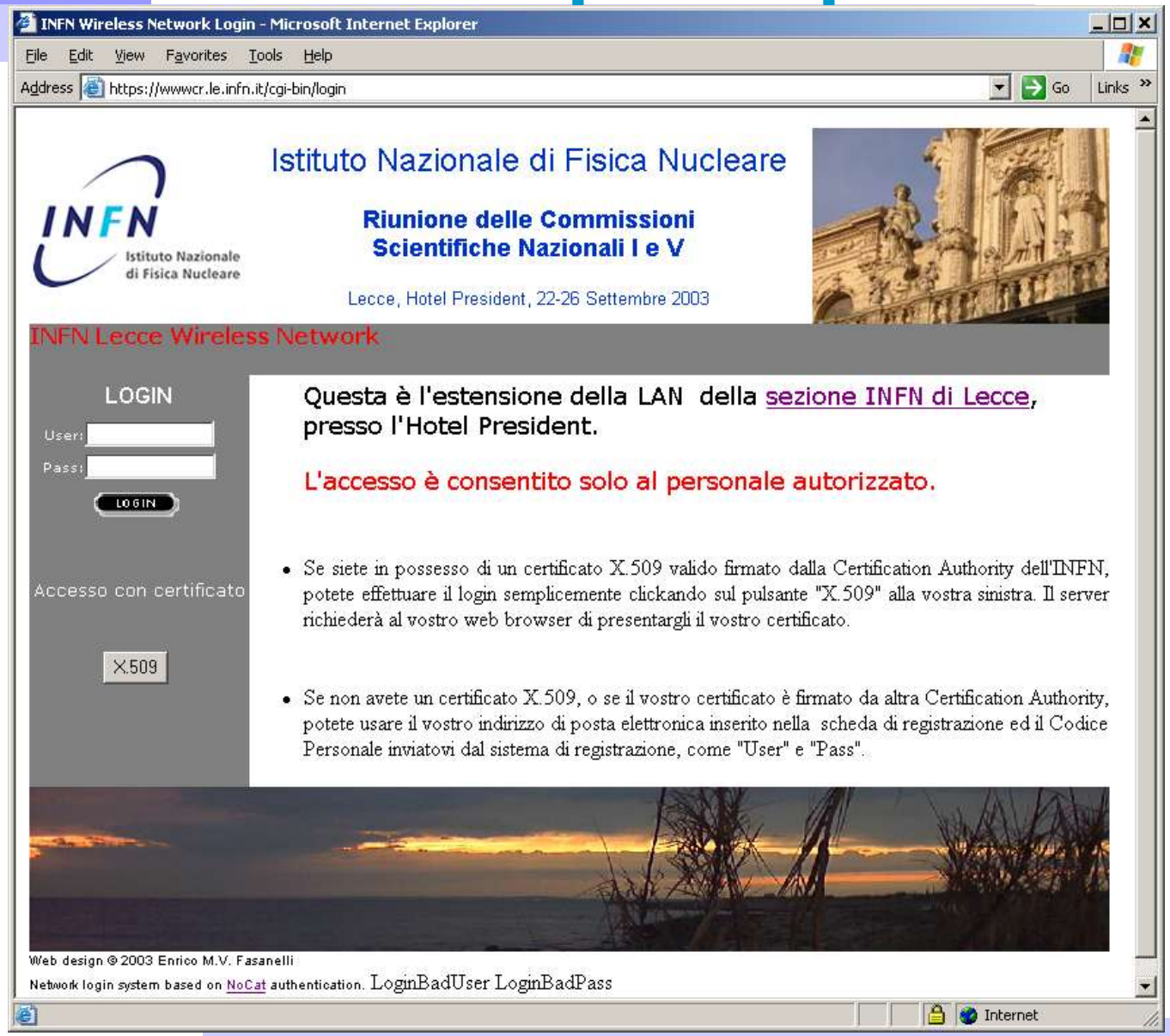
Portale WWW

- Componenti
  - Server web (https), GateWay, Authentication Server
- Il cliente si connette all'AP, ed ottiene un indirizzo IP dal DHCP della VLAN ospiti
- L'indirizzo IP è bloccato dal GW, che intercetta il traffico HTTP e lo dirotta verso l'AS
- Ad autenticazione effettuata, il GW permette il passaggio del traffico

I portali WWW sul mercato

- A pagamento
  - Zyxel B-4000 http://www.zyxel.com/
  - Nomadix Gateway http://www.nomadix.com/
  - Birdstep IP zone http://www.birdstep.com/
  - Cisco BBS ed Authentication proxy
  - Vernier networks (appliance+portal) http://www.verniernetworks.com/
- Free
  - NoCat http://nocat.net/
  - wicap http://www.geekspeed.net/wicap

Il mio primo portale WWW



Network login agent

- Rinnova in modo automatico il network login prima della scadenza
- Permette il Logout (cioè manda un segnale al GW che chiude l'accesso per quel MAC)

Autenticazione

- NoCat Authentication (modificata) nel “test” iniziale (cns I-V settembre 2003)
  - Coppia username/password memorizzata in MySQL DB (e-mail, registration-id)
  - Certificato X.509 firmato dalla INFN CA (verifica del certificato delegata al server apache)
- Considerazioni:
  - esposizione di coppia username/password nella pancia del portale
  - si presta ad attacchi di tipo “social engeneering” via “portal-in-the-middle”

Autenticazione

- La settimana scorsa
  - Via RADIUS (freeradius)
    - EAP-TLS (certificato X.509)
    - PAM (username/password Kerberos5)

Enrico M. V. Fasanelli INFN Sezione di Lecce

To Do

- Test con:
- Autenticazione multipla
  - gli AP Cisco permettono di definire SSID multipli, ognuno associato ad un tipo di autenticazione.
  - Verifica della possibilità di usare una lista di possibili autenticazioni
- EAP-TTLS in freeradius

Enrico M. V. Fasanelli INFN Sezione di Lecce

Conclusioni

- I portali WWW sono veramente usabili da tutti (richiedono solo un web browser ssl-aware)
- Sconsigliato l'uso di username/password (ma non è possibile escluderlo completamente)
- Favorire la diffusione dei certificati X.509

Enrico M. V. Fasanelli INFN Sezione di Lecce