FINALITÀ DEL SEMINARIO

Le reti WiFi hanno subito negli ultimi anni una rapida diffusione: partite come estensioni alle reti aziendali, si sono affermate come mezzo per fornire accesso pubblico a larga banda (hot-spot), fino ad arrivare oggi a una presenza capillare a casa come in automobile, in ufficio come in viaggio.

Il seminario fornirà un quadro completo degli aspetti legati alla sicurezza delle reti WiFi, per comprenderne a fondo vantaggi e rischi.
I partecipanti impareranno a conoscere ed esaminare i problemi di sicurezza specifici alle reti WiFi, insieme alle loro cause e ai mezzi usati per sfruttarli, a valutarne l'impatto sulla sicurezza di un sistema informativo, a confrontare le principali strategie per migliorare il livello di sicurezza delle reti WiFi, a conoscere ed usare le più moderne soluzioni di sicurezza disponibili sia a livello commerciale che di nuovi standard.

Il seminario prevede spiegazioni teoriche intervallate con esempi pratici condotti su una rete WiFi di test.

Programma dettagliato

- Brevi richiami alla tecnologia WiFi: architettura e funzionamento, evoluzione e applicazioni;
- Minacce alle reti WiFi: intercettazione del canale radio, accesso non autorizzato e iniezione del traffico, attacchi al WEP, attacchi a WPA, insicurezza di Radius, minacce all'affidabilità delle reti WiFi;
- Protezione del traffico: crittografia del canale radio con WEP e WPA, utilizzo di reti private virtuali e IPSec, livelli di sicurezza e costi delle diverse soluzioni supportate;
- Controllo degli accessi: credenziali utente basate su password e certificati digitali, il protocollo RADIUS, interazione tra server RADIUS e database utenti, utilizzo di un portale di autenticazione via web;
- Monitoraggio: strumenti per la valutazione della sicurezza in reti WiFi, rilevamento di problemi e attacchi;
- Configurazione sicura di una rete WiFi in rapporto alle diverse esigenze di una sistema informativo.

DESTINATARI

Il seminario si rivolge a chi si occupa di progettazione, gestione e organizzazione di sistemi informativi che sfruttano la tecnologia WiFi e quindi in primo luogo a Progettisti e Amministratori di rete, Responsabili della sicurezza. Risulta utile anche a Progettisti e Responsabili di servizi e

applicazioni per terminali WiFi e per chiunque sia interessato ad approfondire la conoscenza delle moderne tecnologie wireless e della loro sicurezza.

ESPERTO

- **Marco Aime**, Dipartimento di Automatica e Informatica, Politecnico di Torino

Laureato in Informatica e Dottore di Ricerca in Ingegneria Informatica e dei Sistemi, è Assegnista di Ricerca presso il Politecnico di Torino.
Svolge la sua attività all'interno del gruppo di sicurezza Torsec del Dipartimento di Automatica e Informatica e si occupa di sicurezza delle reti wireless, trusted computing, sicurezza delle infrastrutture critiche.
Ha partecipato a vari progetti Europei nel campo della sicurezza dei sistemi informativi, quali TESI, POSITIF, OpenTC, DESEREC.

PARTE SPERIMENTALE

Nell'ambito del seminario verranno svolte parti sperimentali mirate a verificare quanto descritto teoricamente.
La sperimentazione riguarderà l'access point software HopenAP e access point commerciali, il server Radius Freeradius, e il supporto WiFi dei client Windows e Linux.
Durante la sperimentazione saranno utilizzati diversi strumenti per dimostrare l'efficacia di attacchi e contromisure.

MATERIALE FORNITO

Oltre a una copia delle slide usate nel corso, verrà fornito un CD contenente i programmi usati per dimostrare l'efficacia di attacchi e contromisure.

DATE

Chat: Giovedì 08 giugno 2006
Seminario: Giovedì 15 giugno 2006

SCADENZA ISCRIZIONI

Martedì 06 giugno 2006

COSTO

Il costo del seminario è di 350.00 Euro + IVA.
La quota di iscrizione comprende la partecipazione al seminario, la consegna del materiale didattico e del CD, due coffee break e il pranzo, la possibilità di avere un contatto preliminare con il docente tramite chat e quella di contattare con modalità simili il docente in un momento successivo al seminario.