Enginyeria de Telecomunicació, 2n semestre, 2006-2007. *Codi 26118*
Escola Tècnica Superior d'Enginyeria

Professors:

Teoria

Joan Borrell

- Consultes presencials: Dimarts de 12 a 13 i de 18 a 19 al despatx QC-2013
- Consultes virtuals: Email: jborrell@deic.uab.es

Pràctiques

Maria Carmen de Toro

- Consultes presencials: Dimecres de 10 a 11 i de 17 a 18 al despatx QC-2017
- Consultes virtuals: Email: mc@deic.uab.es

Objectius:

L'objectiu del curs és cobrir la teoria i la pràctica del que podríem anomenar, en curt, seguretat en xarxes TCP/IP, és a dir, internets i intranets. El nivell del curs està dissenyat per cobrir els aspectes rellevants en el camp de la seguretat en totes les capes dels protocols de la família TCP/IP, protocols que regulen el funcionament d'aquestes xarxes.
Internet ha estat tradicionalment un mitjà obert i insegur. Les estructures client-servidor o, recentment, els agents mòbils i les aplicaciones entre parells, han revolucionat el mon de la computació i de les comunicacions. La disponibilitat dels serveis, la capacitat de càlcul i d'administració de negoci utilitzant tecnologies basades en navegadors i en el w3 han permès als usuaris un fàcil accés a la informació que, físicament, està ubicada en llocs remots del planeta. La seguretat en la utilització d'una estructura distribuïda ha esdevingut cada dia més important i més complexa tan a nivell de disseny com a nivell d'implementació.
En aquest curs volem donar, en primer lloc, les bases criptogràfiques que permeten entendre la implementació d'uns protocols de seguretat que donen solucions adequades al problema. Estudiarem els principis criptogràfics bàsics, el substracte matemàtic adequat, les primitives criptogràfiques, els algorismes i els protocols criptogràfics que ens donaran solucions a molts dels problemes de seguretat existents en les xarxes. En segon lloc, el curs pretén oferir els elements necessaris per comprendre els diferents atacs possibles als protocols TCP/IP i les mesures de protecció i les de reacció davant aquests atacs, tant criptogràfiques com de filtratge de dades.

Programa:

1. Introducció a la seguretat
    - Valors, riscos i mesures de protecció
    - Aspectes socials i legals
    - Metodologies d'avaluació de la seguretat
    - Sistemes criptogràfics
2. Coneixements previs aritmètics.
3. Criptografia de clau privada.
    - Xifratges en fluxe i en bloc
    - Criptografia clàssica (fins a la segona guerra mundial).
    - Estàndards de xifratge: DES, AES
    - Estàndards i Aplicacions
4. Criptografia de clau pública.
    - Criptosistema RSA i altres
    - Funcions resum o de Hash
    - Signatures digitals.
    - Infraestructures de clau pública (PKI).
5. Protocols criptogràfics
    - Protocol de tres passes de Shamir
    - Protocols d'Administració de claus.
    - Protocols d'Autenticació.
6. Atacs contra xarxes TCP/IP
    - Vulnerabilitats a nivell de xarxa, transport i aplicació
    - Activitats prèvies a un atac
    - Descripció dels atacs més coneguts
7. Mecanismes de prevenció i protecció de la informació
    - Mecanismes a nivell de xarxa: Tallafocs, Xarxes privades virtuals, IPsec
    - Mecanismes a nivell de transport: SSL/TLS
    - Mecanismes a nivell d'aplicació: SSH
8. Mecanismes de detecció i reacció contra atacs i intrusions
    - Sistemes de detecció d'intrusions
    - Sensors, analitzadors, unitats de resposta

Pràctiques:

Hi haurà sis sessions de pràctiques al laboratori del departament d'Enginyeria de la Informació i de les Comunicacions, Q5-2009, els dimarts, de 18:00 a 20:30.

- L'assistència a les sessions de pràctiques és obligatòria.
- Per poder accedir al laboratori cal lliurar, de forma individual, l'informe previ que acompanya l'enunciat. No presentar aquest informe impossibilitarà l'accés al laboratori, i quedarà la pràctica suspesa.
- Per cada pràctica s'haurà de lliurar obligatòriament, de forma individual, un informe final, una setmana després de la sessió de

pràctiques.
- Els subgrups de pràctiques seran de una o dues persones.
- Cal que us apunteu de forma individual a l'únic grup de pràctiques. Per poder-ho fer cal que previament us hagueu registrat en la web del departament.
- Les pràctiques són un 20% de la nota final de l'assignatura
- No hi ha segona convocatoria per a les pràctiques.

Sessions

Sessió	Data	Contingut
1	17-04-2007	PKI
2	24-04-2007	PGP
3	08-05-2007	OpenSSL
4	15-05-2007	SSH + Firewalls
5	22-05-2007	Atacs a xarxes
6	29-05-2007	Mecanismes de prevenció d'atacs

Bibliografia:

- Rifà, J.: *Seguretat Computacional*. Materials, 21. Servei de Publicacions de la UAB (1998).
- Ramió, J., Miret, J.M.: *Libro Electrónico de Seguridad Informática y Criptografía, v.4.1, Publicaciones Universidad Politécnica de Madrid (2006). http://www.criptored.upm.es/guiateoria/gt_m001a.htm*
- *Stallings, W.: Fundamentos de Seguridad en Redes. , Pearson Prentice Hall (2004).*
- *Comer, D.E.: Internetworking with TCP/IP, vol I, 4th ed. , Prentice Hall (2000).*

Avaluació:

Avaluació de l'assignatura: L'avaluació de l'assignatura serà contínua, en dues parts, teoria i pràctiques, que caldrà aprovar per separat.
Avaluació de la teoria: Durant la primera convocatòria, cada setmana hi haurà un problema o activitat proposada que haurà de ser resolt de forma individual per cada alumne i lliurat al professor a través de l'espai wiki (https://wiki.uab.es/0607-ET-CSX) de l'assignatura per fer un portafoli virtual de l'assignatura. Altres activitats (treballs d'ampliació del temari per exemple) seran optatives. Els alumnes que no hagin lliurat satisfactòriament un mínim del 70% dels problemes i/o activitats obligatoris de la primera convocatòria hauran d'anar a la segona convocatòria, on, a part d'haver de lliurar satisfactòriament un mínim del 50% dels problemes i/o activitats obligatoris de la primera convocatòria, hi haurà un examen escrit. La nota de teoria serà el

80% de la nota final.

Avaluació de les pràctiques:

- Les sessions de pràctiques són d'assistència obligatòria.
- Cada pràctica s'avalua pel seu previ i informe final. Aquest documents s'han de fer de forma individual.
- Cal aprovar les pràctiques per aprovar l'assignatura. Es fa mitja de pràctiques a partir d'un cinc.
- La nota de pràctiques és el 20% de la nota final, i s'obté per la mitjana ponderada de les notes de les diferents pràctiques.
- No hi ha segona convocatòria per a les pràctiques.