DNS

Orice dispozitiv de calcul in retea, capabil sa comunice cu alte dispozitive, este identificat cu o adresa IPv4 unica. (adresa IPv4 = 32 biti)
Fiecare gazda primeste un nume. Cand vrem sa comunicam cu o gazda, folosim numele ei. Trebuie facuta legatura intre numele gazdei si adresa IP. Asocierea se facea printr-un fisier text (domeniu plat de adrese) dar s-a constatat ca e o metoda incomoda.

Spatiu de nume DNS

- gazdele din retea au fost impartite in grupe: generice (gov, edu), tari (ro, jp), etc.
- structura arborescenta
- frunzele = gazdele in retea
- pe acelasi nivel, domeniile trebuie sa aiba nume diferite
- numele absolut al domeniului = parcurgerea drumului pana la radacina (info.uaic.ro)
- nume relativ (edu)

Inregistrari de resurse (RR = resource records)

- fiecarui nod i se atribuie informatii (RR-uri)

Nume domeniu	TTL (Time-to-live, exprimat in secunde)	Clasa (IN = Internet)	Tip (SOA = Start of Authority, A = Address, NS = Name server, MX = Mail exchanger)	RLength	RData

SOA = inceputul unei zone de autoritate
A = adresa IP a gazdei
NS = server de nume cu autoritate pe domeniu
MX = informatii despre e-mail (server de e-mail)

Zone de autoritate

- spatiul de nume DNS nu poate fi gestionat de numai o singura zona de autoritate
- este impartit in subzone de autoritate
- domeniile de pe nivelul intai = zone de autoritate. Cand o zona de autoritate se divide, ea deleaga autoritate copiilor

DNS

- stabileste legatura intre numele gazdei si o anumita informatie asociata nodului (de exemplu adresa IP)
- rezolutia numelui de domeniu se realizeaza printr-un program numit resolver
- există 2 tipuri de rezolutie de nume: rezolutie recursiva (name resolverul cere serverului de nume sa faca translatarea) si rezolutie iterativa (name resolverul cere serverului de nume sa ii furnizeze adresa IP a unui server care poate face translatarea)

DNSSec

- atacuri asupra DNS - lipsa autentificarii originii si a unei metode de stabilire a integritatii datelor
- 4 tipuri de inregistrari cu scopul: - de a semna informatiile din arborele DNS
  - de a identifica chei de obtinere a semnaturii
  - de a returna raspuns in cazul esuarii rezolutiei
  - de a identifica originea

1. DNSKey - cheie de verificare a semnaturii

Flags (256)	Protocol (3 - DSA, SHA-1)	Algoritm (5)	Cheie publica (RSA)

Flags = ver. daca cheia publica e folosita pentru verificarea semnaturilor pe inregistrari (256)

2. RRSIG - folosit pentru a semna si autentifica RR-seturile. Specifica un interval de validitate pentru semnatura
   - pentru un grup de inregistrari de acelasi tip
   - cheia pentru verificarea semnaturii din zona RR se gaseste intr-o inregistrare de tip DNSKey
   - se determina pornind de la informatiile din zona RRSIG (de la algoritmul utilizat, campul Tag si numele semnatarului)

3. NSEC

Next domain	BitMaps

- ne da urmatoarea zona de autoritate, in ordine canonica

4. DS
   - contine o functie hash asupra cheii (publice) din DNSKEY-ul de pe nivelul inferior, pentru validarea semnaturii
   - se construieste un lant de incredere -> mecanismul de autentificare a originii in DNS

SSL/TLS (Secure Sockets Layer/Transport Layer Security)

Care este scopul de baza a protocolului SSL/TLS?

- scopul de baza al acestui protocol este de a asigura unui canal de comunicare confidentialitatea datelor, autentificarea partilor si integritate.
- orientat pe socketi (datele sunt impachetate in acelasi mod)

SSL handshake protocol	SSL change cipher protocol	SSL alert protocol	HTTP
SSL record protocol			
TCP			
IP			

SSL record protocol = pentru transferul de date

TLS reprezinta o incercare de a produce un standard Internet al SSL. Diferentele fata de SSL sunt:
- scheme de MAC diferite
- generarea secretului master prin utilizarea unor functii pseudo-random
- se utilizeaza criptografie pe curbe eliptice
- sunt adaugate coduri de alerta

Descrieti metodele de schimb de cheie RSA si DH in SSL.

- RSA -> clientul genereaza un secret pre-master care e criptat cu cheia publica a serverului. In acest caz, un certificat public de cheie pentru cheia serverului trebuie sa fie disponibil.

- DH -> Fixed-DH - serverul trebuie sa aiba un certificat ce include parametrii lui DH publici
  - clientul isi pune la dispozitie parametrii sai DH publici printr-un certificat sau printr-un mesaj de schimb de chei
  -> Ephemeral (temporary, one-time)-DH - parametrii publici DH sunt schimbati si semnati, folosind cheia privata RSA sau DSS a expeditorului
  - este nevoie de certificate pentru a autentifica cheile publice
  -> Anonymous-DH - fara nicio autentificare

Care sunt pasii de baza ai protocolului "SSL record"?

E protocolul ce permite ca toate mesajele aplicatiei sa fie transmise. Pasii de baza ai protocolului:
- preia un mesaj ce trebuie transmis
- il fragmenteaza in blocuri (<= 2^14 bytes)
- optional comprima blocurile
- aplica MAC pe fiecare bloc -> confidentialitate si integritate a mesajului
- cripteaza fiecare bloc
- adauga un header SSL
- transmite rezultatele intr-un segment TCP

Datele primite sunt procesate in ordine inversa

Generarea cheii pre-master
- in cazul RSA - clientul genereaza un secret pre-master, il cripteaza cu cheia publica RSA a serverului si o trimite serverului. Serverul decripteaza mesajul si extrage secretul pre-master
- in cazul DH - si clientul si serverul isi trimit unul altuia valoarea publica DH si apoi computeaza (acelasi) secret pre-master

TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP este cel mai utilizat protocol folosit în retelele locale cat si pe Internet datorita disponibilitatii si flexibilitatii lui avand cel mai mare grad de corectie al erorilor. TCP/IP permite comunicarea intre calculatoarele din intreaga lume, indiferent de sistemul de operare instalat.
Protocolul este compus din patru niveluri: Aplicatie, Transport, Retea si Acces la retea.

IP (Internet Protocol)

Protocolul Internet este o metoda sau un protocol prin care datele sunt trimise de la un calculator la altul prin intermediul Internetului. Fiecare calculator (cunoscut sub denumirea de "gazda"), are pe Internet cel putin o adresa IP unica, care il identifica intre toate computerele din retea. Cand cineva trimite sau primeste informatii (de ex.: posta electronica, pagini web) mesajul este impartit in blocuri de mici dimensiuni denumite pachete. Fiecare pachet cuprinde adresa expeditorului si pe cea a destinatarului.

TCP (Transmission Control Protocol)

Protocolul de control al transmisei este folosit de obicei de aplicatii care au nevoie de confirmare de primire a datelor. Efectueaza o conectare virtuala full duplex intre doua puncte terminale, fiecare punct fiind definit de catre o adresă IP si de catre un port TCP (numar pe 16 biti).
Opereaza la nivelul transport, avand urmatoarele caracteristici:

- orientat pe conexiune
- punct la punct
- fiabil
- permite o comunicare inter-procese intre perechi de procese aflate in retele distincte, dar conectate.

Un port este punct de comunicatii care faciliteaza schimbul de informatii intre unul sau mai multe calculatoare. Pe un computer putem avea intre 0 si 65535 de porturi asociate unor anumite task-uri.

IPSec

Arhitectura de securitate pentru protocolul de Internet (IPv4 si IPv6) care furnizeaza serviciile de securitate la nivelul IP-ului, prin permiterea unui sistem de a selecta protocoalele de securitate necesare; determina algoritmii folositi pentru serviciu, pune in ordine orice chei criptografice necesare pentru accesarea serviciilor dorite.

Ce este o asociere de securitate in IPSec si care sunt mecanismele de securitate fundamentale din IPSec?

O asociere de securitate (SA) este o conexiune logica si unidirectionala intre 2 sisteme IP, identificate unic prin tripletul (SPI, adresa IP destinatie, protocolul de securitate)

SPI (Security parameter index) - este o valoare pe 32 de biti, folosita pentru a identifica diferite SA-uri cu aceeasi adresa destinatie si acelasi protocol

adresa IP destinatie - poate fi unicast, broadcast sau multicast. Mecanismele de management curente ale SA sunt definite doar pentru adrese unicast

protocol de securitate - poate fi AH sau ESP

Mecanisme fundamentale:

1. Protocoale de securitate:
    - AH (Authentication Header) - asociat unei datagrame IP, pentru autentificarea unor campuri din datagrama
    - ESP (Encapsulating Security Payload) - obtinut din datagrama IP prin criptarea si optional autentificarea unor campuri din datagrama
2. Asocieri de securitate (SA)
3. Key management (manual si automatic)
4. Algoritmi pentru autentificare si criptare

Servicii oferite - access control, conectionless integrity, data origin authentication, rejection of replayed packages, confidentiality, limited traffic flow confidentiality

Descrieti protocolul AH in cele 2 moduri de utilizare pentru datagrame IPv4

IP header	TCP segment

->(apply AH)

IP header	AH	TCP segment	(transport mode)
New IP header	AH	IPv4 datagram	(tunnel mode)

Modul transport - AH autentifica doar corpul (fara header) datagramei, eventual portiuni din header
- campurile mutabile nu vor fi autentificate

Modul tunel - AH autentifica intreaga datagrama (se aduce un header suplimentar)

Descrieti protocolul ESP in cele 2 moduri de utilizare pentru datagrame IPv4

IP header | TCP segment ->(apply ESP) IP header | ESP header | TCP segment | ESP trlr | ESP auth (transport mode)

New IP header | ESP header | IPv4 datagram | ESP trlr | ESP auth (tunnel mode)

Modul transport - ESP cripteaza doar corpul datagramei (nimic din header)

Modul tunel - ESP cripteaza intreaga datagrama (cu tot cu header) si va trebui un alt header
- se incapsuleaza tot - se pune in noi headere

Descrieti cateva combinatii de asocieri de securitate in IPSec.

-end-to-end - doua gazde sunt conectate prin Internet sau intranet fara o poarta de securitate intre ele. Acestea pot folosi ESP, AH sau ambele. Pot fi aplicate oricare din modurile transport sau tunel

-VPN - gazdele din intranet nu sunt obligate sa suporte IPSec, dar portile (gateway) sunt obligate sa ruleze IPSec si sa suporte modul tunel (ori cu AH, ori cu ESP)

-end-to-end cu VPN - este o combinatie intre cazurile precedente. De exemplu, portile pot folosi AH in modul tunel, in timp ce gazdele folosesc ESP in modul transport

-remote access - intre gazda si firewall este necesar doar modul tunel, iar intre cele doua gazde poate fi folosit atat modul tunel cat si modul transport

RFC 822 (formatul de e-mail), MIME (Multipurpose Internet Mail Extensions)

Care sunt principalele dezavantaje ale formatului de e-mail RFC 822?

- nu suporta mesaje in limbile cu accent (ex: franceza), in alfabete non-latine (ex: rusa), sau in limbile fara alfabet (ex: chineza)
- nu suporta informatii non-textuale (ex: fisiere grafice, multimedia)
- existau constrangeri in scrierea subiectului: fiecare linie trebuia sa se termine cu caracterele CR si LF
- fiecare linie trebuia sa contina <78 caractere

Care este structura de baza a unui format MIME?

Ideea de baza pentru MIME:
- adauga o structura la corpul mesajului
- codifica date ASCII si date non-ASCII

Pentru a putea oferi informatii despre noile date s-au definit 5 headere noi:
- MIME-version = identifica versiunea MIME
- Content-Description = specifica ce este un mesaj
- Content-ID = identificator unic
- Content-Type = descrie tipul datelor care sunt codate in MIME
- Content-Transfer-Encoding = specifica metoda de codare pentru fiecare parte a corpului

Body-part:
- text/enriched
- image/jpeg
- audio/mpeg
- video/dv
- model/vrml
- application/pdf
- message/rfc822

Care sunt cele 4 metode de codificare a informatiei in MIME?
Codificarea MIME a corpului.
- 7 bit = indica un format 7-bit ASCII
- 8 bit/binary = codare folosind caractere pe 8 biti
- quoted-printable = se foloseste cand majoritatea datelor sunt de tip ASCII si exista putine caractere non-ASCII
- base64 = codeaza datele mapand blocuri de intrare de 6 biti pe blocuri de iesire de 8 biti. (Radix 64)

SMTP (Simple Mail Transfer Protocol)

Protocolul simplu de transfer al corespondentei este un protocol folosit pentru transmiterea mesajelor in format electronic pe Internet. SMTP foloseste portul de aplicatie 25 TCP si determina adresa unui server SMTP pe baza inregistrarii MX (Mail eXchange, "schimb de corespodenta") din configuratia serverului DNS.
POP3 si IMAP sunt protocoalele prin care putem manvera intre serverele de mail si computerul personal mailurile.

PGP (Pretty Good Privacy)

Ce servicii ofera PGP?

PGP este un program care furnizeaza confidentialitate si autentificare criptografica pentru comunicarea cu date.
PGP ofera 2 servicii criptografice:

- autentificare (prin semnaturi)
- confidentialitate (prin criptare)

si 3 servicii auxiliare:

- comprimare (folosita dupa semnarea mesajului, dar inainte de criptare)
- compatibilitate e-mail (conversie base64)
- segmentare (mesajele mai lungi de o lungime maxima data, sunt "rupte" in segmente mai mici)

Cum se realizeaza autentificarea in PGP?

Autentificarea PGP (aplicata lui x):

- sigA(x) este semnatura lui A peste x
- Z = Zip compression
- semnatura lui A poate fi o semnatura RSA sau DSS pe SHA-1(x)

Cum se asigura confidentialitatea in PGP?
Confidentialitate PGP (aplicata lui x):
- A->B:({K})$\{Z(x)\}_k$, $\{K\}_k$ B e (indice B, putere e si k e tot indice)

- criptarea simetrica se face cu CAST-128, IDEA sau 3DES, toate in modul CFB
- criptarea asimetrica se face cu RSA sau ElGamal

Cum se realizeaza autentificarea + confidentialitatea in PGP?
Impreuna, autentificarea si confidentialitatea in PGP se obtine prin aplicarea confidentialitatii pe x'=(x,sigA(x))

Cum se realizeaza compresia informatiei in PGP?
Atat PGP cat si S|MIME folosesc in prezent metoda de compresie ZIP.
Algoritmul de compresie LZ realizeaza compresia prin inlocuirea portiunilor de date cu referinte la date pereche (potrivite) care au trecut deja atat prin codificare cat si prin decodificare. O potrivire este codificata printr-o pereche de numere numite o pereche "lenght-distance", care este echivalenta cu declaratia "fiecare din lungimile de caractere este egala cu caracterul la exact distanta caracterelor in urma in streamul necompresat".

Bi=k*prefix(i)+ultim(i) ex: 1233444455555

Explicati modul de formare si utilizare a inelelor de chei in PGP.

-depozitul de chei PGP este bazat pe asocierea identificatorilor cu cheile publice
-cheile asimetrice sunt stocate ca structuri de tip tabel numite inele de chei, care pot fi indexate dupa user ID sau key ID
-PGP stocheaza doua inele de chei ca doua fisiere pe HDD-ul gazdei: unul pentru chei private, unul pentru chei publice

Forma:
inelul de chei publice contine: stampila de timp, id-ul cheii, cheia publica, id user, +4 campuri care se refera la gradul de incredere in detinatorul cheii si in cheie: owner trust, Key Legitimacy, Signature(s), Signature(s) Trust.

Utilizare:

1. Userul U semneaza un mesaj
- PGP recupereaza cheia privata criptata a lui U din inelul de chei private folosind ID(U).
- PGP ii solicita lui U parola pentru a recupera cheia privata a lui U
- semnatura este construita.
2. Userul U cripteaza mesajul
- PGP genereaza o cheie de sesiune si cripteaza mesajul
- PGP recupereaza cheia publica a destinatarului din inelul de chei publice folosind ID-ul
- cheia de sesiune este criptata cu cheia publica a destinatarului

3. Userul U verifica semnatura
- PGP recupereaza cheia publica a expeditorului din inelul de chei publice, folosind key ID (care este atasat de mesajul primit)
- PGP verifica semnatura

4. Userul U decripteaza mesajul
- PGP recupereaza cheia privata criptata a lui U din inelul de chei publice folosind user ID
- PGP solicita lui U parola ptr a recupera cheia privata a lui U.
- PGP decripteaza mesajul

Cum se realizeaza autentificarea in S/MIME?
1. A->B: R64 (ID pkc, ID mda, ID ea, sig k A d (x),x) (sig, k indice, a indice, d putere a lui K)
-ID pkc: identificatorul certificatului cheii publice a celui care a semnat
-ID mda: identificatorul algoritmului care face rezumatul mesajului x
-ID ea: identificatorul algoritmului de criptare folosit ptr a cripta rezumatul mesajului x/
-R64: Radix 64.

2. Semnatura clear
A->B: R64 (ID pkc, ID mda, ID ea, sig k A d (x'),x')
-x' este obtinut prin codarea lui x cu Radix 64 sau quoted-printable, in cazul in care x nu e 7-bit ASCII.
-cu acest caz mesajul poate fi vazut de oricine are capabilitati MIME, dar nu poate verica semnatura.

3. Cum se asigura confidentialitatea in S/MIME?
A->B: ({k})R64 (ID pkc, ID mda, ID ea, {k}k B e, {x}k) (indice K, indice B, putere e)
-ID pkc: identificatorul certificatului cheii publice a destinatarului (certifica K B e)
-ID ea: identificatorul algoritmului de criptare folosit pentru a cripta cheia de sesiune K

Ce se intelege prin Zero-Knowledge proofs?

In protocolul challenge-and-response, A demonstreaza ca stie un secret. Din punct de vedere al lui B(verifer) exista 2 cazuri:

- in timpul protocolului B afla secretul
- in timpul protocolului B nu afla nimic legat de secret, ci doar faptul ca A stie secretul ->protocolul -> zero-knowledge protocol, iar identificarea dovezii lui A (prover) = zero-knowledge proof.

In ce consta metoda de codificare "quoted printable"?

R1: Orice octet exceptand CR sau LR atunci cand sunt in perechea CRLP poate fi reprezentat prin "=xy" unde x,y sunt cifre in hexazecimal
R2: Orice octet intre 33-60 (zecimal) sau (62-126) poate fi reprezentat prin ASCII pe 7 biti
R3: octetul 9 (tab) si 32 (spatiu) pot fi reprezentati prin codurile lor ASCII daca nu sunt la sfarsitul liniei, altfel se aplica regula 1
R4: Separatorul de linie e perechea CRLF; daca CRLF nu functioneaza ca un separator de linie atunci "=0D=0A"
R5: Daca linia depaseste 76 caractere, atunci se insereaza un asa numit "soft break" la coloana 75 sau inainte de coloana 75

In ce consta metoda de codificare Radix 64?

Pas 1: pentru fiecare caracter din textul initial, se reprezinta in baza 2 codul sau ASCII
Pas 2: se concateneaza toate reprezentarile caracterelor
Pas 3: intr-un buffer se iau blocuri de cate 3 octeti (24 biti)
Pas 4: pachete de cate 6 biti (din buffer) se transforma in 4 numere
Pas 5: se codifica cele 4 numere cu valorile corespunzatoare din Base64