2. SNMP este un protocol rutabil întrucât folosește protocolul IP pentru încapsularea datelor și, implicit, adresarea IP.

3. Există și protocoale de management al rețelelor locale de calculatoare, nerutabile. Un astfel de protocol este NetBeui (*Network BIOS extended user interface*), dezvoltat de firma Microsoft pentru rețele Netware (de PC-uri), cu sistem de operare NT, pe baza modelului client-server. Pe lângă operațiile de management de rețea, NetBeui include și funcțiile de transport, de corecție a erorilor de transmisie, de confirmare a recepției corecte a datelor (ACK), fiind echivalent unei stive de protocoale cu funcții distincte. Toate acestea determină o creștere considerabilă a timpului de transmisie a pachetelor și apariția blocajelor în rețea cauzate de așteptarea unor mesaje de confirmare pierdute. O altă limitare a NetBeui este aceea dată de numărul maxim admis de sesiuni simultan deschise în rețea (254). Aceste dezavantaje ale NetBeui sunt eliminate în cadrul protocolului NBF (*NetBeui Frame*), cu 'fereastră glisantă' de transmisie (*sliding window*).

II.1.12 Protocoale de securitate în Internet

Securitatea comunicațiilor în rețelele locale de calculatoare se referă la mai multe aspecte:

1. mesajele transmise provin din surse autorizate și sunt autentice;

2. datele sunt corecte și complete;

3. accesul la anumite mesaje cu caracter confidențial este restricționat în mod corespunzător.

Există diferite metode de asigurare a securității transmisiei într-o rețea prin operații de autentificare a utilizatorilor, criptare a mesajelor, filtrare a traficului etc.

Metodele de securitate din Internet se pot aplica pe diferite nivele ale modelului OSI.

La nivel fizic, se pot folosi module hardware de criptare și decriptare (ENCO).

La nivelul legăturii de date și la nivel de rețea se pot defini filtre de includere sau de excludere pe diverse interfețe ale echipamentelor.

Se pot utiliza programe de aplicație specializate pentru asigurarea securității transmisiei datelor în rețea.

Primele măsuri de securitate a rețelelor defineau **asociații de securitate** (SA - *Security Association*), adică grupuri de utilizatori autorizați să folosească o anumită rețea, denumită **rețea virtuală privată** (VPN - *Virtual Private Network*).

În prezent, în rețelele TCP/IP se utilizează suita de protocoale de securitate **IPsec** (*Internet Protocol Security Facility*), care realizează criptarea și autentificarea pachetelor IP cu performanțe

superioare sistemului inițial SA. VPN pot fi configurate în mod adecvat să aplice protocoalele de securitate din suita IPsec.

Gradul de protecție a pachetelor IP și cheile de criptare utilizate de IPsec se stabilesc prin mecanismul IKE (*Internet Key Exchange*), care se aplică folosind protocolul ISAKMP (*Internet Security Association and Key Management Protocol*). Astfel IPsec beneficiază de serviciile ISAKMP/IKE.

IPsec oferă următoarele servicii de securitate pe nivelul IP al rețelelor TCP/IP:

1. **integritatea conexiunii** - asigură faptul că în procesul de comunicație nu intervin entități neautorizate care să modifice datele sau să genereze mesaje false în rețea;

2. **autentificarea sursei de date** - permite identificarea sursei și asigurarea autenticității mesajelor;

3. **criptarea datelor** - asigură confidențialitatea mesajelor transmise și imposibilitatea preluării neautorizate a informațiilor;

4. **protecția la atacuri în rețea** - detectează pachetele repetitive, replici ale aceluiași pachet, care se transmit la infinit în rețea și pot produce blocaje sau saturarea rețelei (*flooding*).

Autentificarea sursei se face pe baza protocolului AH (*IP Authentication Header*) din suita IPsec (RFC 2401, RFC 2402). Acest protocol asigură integritatea conexiunii și a datelor transmise, precum și autenticitatea mesajelor. AH asigură securitatea integrală a pachetelor IP, inclusiv antetelor de securitate atașate ulterior acestora.

Serviciile de securitate sunt asigurate și de protocolul ESP de încapsulare a pachetelor IP (*IP Encapsulating Security Payload*), care stabilește operații de criptare a datelor și de autentificare a sursei de informații (RFC 2406).

ESP oferă servicii de securitate numai protocoalelor de pe nivelele superioare celui de rețea, excluzând antetele de securitate ulterior adăugate pachetelor.

Protocoalele AH și ESP pot fi implementate prin diverși algoritmi software și se pot aplica fie individual, fie ambele simultan, în funcție de gradul de securitate impus pachetelor IP (RFC 2403, RFC 2404).

IPsec asigură securitatea comunicației dintre două calculatoare-gazdă, dintre două echipamente de comunicații (de exemplu, rutere) sau dintre un DTE și un DCE.

Un router sau un server pe care sunt activate protocoalele de securitate IPsec se numește **poartă de securitate** (*security gateway*) sau **"zid" de protecție** (*firewall*).

În general, asigurarea securității unei transmisii se realizează la ambele capete ale căii de comunicație, cu două echipamente care folosesc IPsec lucrând în pereche (*IPsec peers*).

Cele două protocoale de securitate în Internet (AH sau ESP) pot acționa în două moduri:

1. **modul de transport** - protocolul de securitate intervine în pachetul IP și adaugă un antet de securitate imediat după antetul IP (cu sau fără opțiuni exprimate). ESP oferă protecție numai protocoalelor de nivel superior, în timp ce AH securizează total pachetul, inclusiv antetul IP.

2. **modul de tunelare** (*IP tunneling*) - se introduc două antete de securitate în fiecare pachet, înainte (*outer header*) și după (*inner header*) antetul IP. Antetul extern specifică perechea de entități între care se creează tunelul IP și se aplică măsurile de securitate pe baza IPsec. Antetul intern precizează destinația finală a pachetului. ESP protejează numai pachetul transmis prin tunelul IP, în timp ce AH asigură și securitatea antetului exterior atașat.

Configurarea echipamentelor dintr-o rețea în vederea aplicării IPsec se realizează de către o persoană cu drepturi depline de stabilire a securității rețelei (*security officer*), în trei etape:

1. crearea grupurilor de securitate (SA) și stabilirea drepturilor și atribuțiilor acestora;

2. configurarea legăturilor dintre SA-uri și stabilirea ierarhiilor de priorități, folosind ISAKMP/IKE (RFC 2408, RFC 2409);

3. stabilirea modalităților de clasificare a pachetelor IP și de acțiune asupra lor (permite sau interzice accesul în rețea, aplică procedurile de securitate conform IPsec).

Aceste configurații referitoare la IPsec sunt stocate în bazele de date pentru securitatea rețelei (SPD - *Security Policy Database*), la care are acces doar administratorul de rețea.

Prin SA înțelegem o conexiune simplex definită pe o pereche IPsec, pentru securitatea traficului doar într-un sens, folosind un singur protocol de securitate (AH sau ESP).

Pentru transmisiile duplex se definește câte un SA pentru fiecare sens de comunicație cu rețeaua (*inbound/outbound traffic*).

Dacă la unul din capetele canalului de comunicație definit de SA, se găsește un echipament de securitate (*security gateway; firewall*), atunci este obligatoriu ca acel SA să lucreze în modul de tunelare pentru a evita problemele create prin fragmentarea pachetelor și de existența căilor multiple de rutare.

Un SA este identificat prin trei parametri:

1. un număr aleator denumit **identificator de securitate** (SPI - *Security Parameter Index*);

2. **adresa IP de destinație;**

3. protocolul de securitate (AH sau ESP).

Dacă este necesară utilizarea ambelor protocoale de securitate în Internet (AH și ESP), atunci se creează și se configurează legăturile dintre două sau mai multe SA.

Regulile de securitate aplicate într-o rețea folosind IPsec sunt memorate în SPD. Acestea stabilesc trei moduri posibile de acțiune asupra pachetelor IP:

1. se aplică pachetului, serviciile de securitate conform IPsec;

2. se interzice accesul pachetului în rețea (*deny*);

3. se acordă permisiunea de acces în rețea, fără aplicarea măsurilor de securitate IP (*bypass IPsec*).

Modul de acțiune asupra unui pachet IP se stabilește pe baza antetelor conținute de acesta, prin operația de clasificare a pachetelor, în funcție de diverși **factori de selecție**:

- adresa IP a sursei;
- adresa IP a destinației;
- portul-sursă;
- portul-destinație;
- protocolul de transport;
- numele utilizatorului sau al sistemului;
- gradul de prioritate a informațiilor conținute în pachet.

Aplicarea măsurilor de securitate IPsec asupra unui pachet (autentificare, criptare, compresie), se realizează pe baza mecanismului ISAKMP/IKE prin care se generează și se transmit între părți cheile de criptare utilizate de SA în diferite sesiuni, memorate într-o bază de date proprie ISAKMP ca atribute ale SA.

În rețelele TCP/IP, se utilizeazează diverși algoritmi de criptare, uzuali fiind cei cu cheie publică (RSA, Diffie-Hellman, DES, 3DES etc).

De exemplu, protocolul SSH, utilizat pentru transferul securizat al fișierelor și al mesajelor prin sistemul de poștă electronică din Internet, folosește diverși algoritmi de criptare cu cheie publică. Operația de autentificare se bazează de asemenea pe secvențe de tip 'cheie de transmisie'.

APLICAȚII

1. Încărcați de pe Internet și analizați cele mai recente documente RFC referitoare la protocoalele din suita TCP/IP.
2. Lansați în execuție diferite programe de aplicații de tip poștă-electronică și de transfer a fișierelor. Observați performanțele fiecăruia.
3. Aplicați diferite comenzi specifice protocoalelor din suita TCP/IP și observați efectele acestora precum și codurile de răspuns generate.
4. Studiați algoritmii de criptare a datelor în Internet (DES, IDEA, RSA) și faceți o comparație a performanțelor acestora.
5. Testați conexiunile dintre diferite noduri din rețeaua locală, eventual și din Internet.
6. Deduceți rutele de acces dintre diverse servere din Internet.