Prof.Dr. Ferucio Laurenţiu Ţiplea
Facultatea de Informatică
Univ. "Al.I.Cuza", Iaşi

Curs: Securitatea Informaţiei

Săptămâna 6 – 9

Tema nr. 3: Centru de distribuţie de chei

Considerăm următorul protocol prin care un utilizator U se adresează unui server de încredere T pentru a obţine o cheie de accesare a unui serviciu de reţea S (se presupune că atunci când U şi S se înregistrează pentru prima dată în reţea, ei vor obţine cheile de comunicare cu T notate K_{UT} şi, respectiv, K_{ST}, pentru un acelaşi criptosistem $\mathcal{S}$ fixat):

1. Atunci când U doreşte să acceseze servicul S, ceea ce se poate face numai cu o cheie validă, el se adresează serverului T cu un mesaj de forma

   $$U, S, n_1$$

   unde n_1 este un *nonce* (element random generat). Acest mesaj îi spune lui T că el, U, doreşte o cheie pentru a accesa S, iar n_1 este un identificator al acestei sesiuni de comunicaţie;

2. Serverul T verifică identitatea lui U cât şi dreptul acestuia de a accesa S şi, dacă aceşti paşi se încheie cu succes, generează o cheie K şi transmite lui U mesajul

   $$\{K, n_1, L, S\}_{K_{UT}}, \{K, U, L\}_{K_{ST}}$$

   unde L este durata de viaţă a cheii (de exemplu, 2 ore). Prima parte a mesajului, criptată cu cheie K_{UT}, se adresează lui U, permiţându-i acestuia să extragă cheia K de acces la S, cu durata ei de viaţă (prezenţa lui n_1 în acest mesaj identifică sesiunea şi confirmă lui U că respectiva cheie K este pentru sesiunea iniţiată de el în care a folosit n_1). Partea a doua a mesajului se adresează lui S şi ea va fi transmisă lui S de către U;

3. Când U primeşte mesajul de mai sus de la T, va decripta prima parte a mesajului, va verifica n_1 şi S raportate la mesajul transmis de el şi, dacă verificarea se încheie cu succes, va transmite lui S mesajul

   $$\{K, U, L\}_{K_{ST}}, \{U, t_U, L\}_K$$

   Prima parte a mesajului provine din mesajul lui T către U, iar a doua parte are ca scop confirmarea cheii K (t_U este o ştampilă de timp);

4. Când S primeşte mesajul de la U, va decripta prima parte a acestuia, va extrage cheia K, va decripta a doua parte a mesajului şi va face următoarele verificări: identitatea utilizatorului din prima parte a mesajului corespunde cu identitatea utilizatorului din a doua parte a mesajului, ştampila de timp este validă, iar timpul curent se încadrează în durata L de viaţă a cheii. Dacă acestea se încheie cu succes, S va răspunde cu

$$\{t_U, L-1\}_K$$

ce va confirma lui U faptul că U şi S folosesc aceeaşi cheie K.

Dacă cei patru paşi de mai sus se finalizează cu succes, comunicarea între U şi S se va face cu cheia K ce are durata de viată L.

Se cere implementarea unui centru de distribuţie de chei, folosind protocolul de mai sus, cu următoarele specificaţii:

1. criptosistemul $\mathcal{S}$ este 3DES cu 3 chei diferite, sau AES (lungimea cheii va fi de 192 bits);
2. U şi S vor comunica cu 3DES cu 2 chei diferite (lungimea cheii va fi de 128 bits);
3. Generarea de chei pentru U şi S se va face cu un generator existent în mediul de programare;
4. T va implementa o politică de tip Bell-LaPadula de acordare a accesului la servicii (utilizatorii vor avea nivele de securitate, iar serviciile fi clasificate).