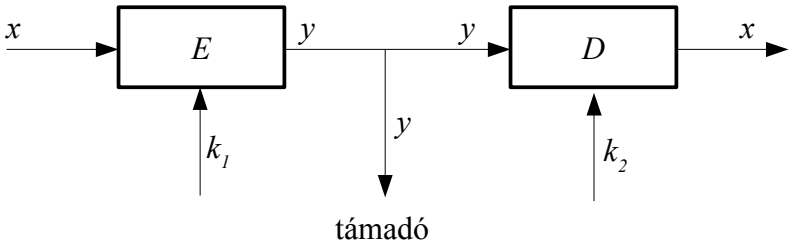
Kriptográfiai alapfogalmak

A kriptológia a titkos kommunikációval foglalkozó tudomány. Két fő ága a kriptográfia és a kriptoanalízis. A kriptográfia a titkosítással foglalkozik, a kriptoanalízis pedig a titok jogosulatlan megfejtésével. A titkos kommunikáció modellje a következő.



1. ábra: A rejtjelezés modellje

A szeretné az *x* üzenetet egy nyilvános csatornán keresztül eljuttatni **B**-nek úgy, hogy a nyilvános csatornán hallgatózó támadó az üzenet tartalmát ne ismerhesse meg. (A támadó a kommunikáció tényéről tudomást szerezhet.) Ennek érdekében az *x nyílt szöveg*ből (plain text) az $E_{(k_1)}(.)$ *rejtjelező transzformáció*val a k_1 *kulcs* (key) használatával elkészíti (encryption) az *y rejtett üzenet*et (cipher text):

$$y = E_{(k_1)}(x)$$

A k_1 tetszőleges rögzített értéke mellett $E_{(k_1)}(.)$ kölcsönösen egyértelmű leképzés. Úgy is mondhatjuk, hogy a lehetséges *E* transzformációk halmazából a k_1 kulcs jelöli ki azt, amelyiket éppen

alkalmazzuk. A nyilvános csatornán hallgatózó támadó az *E* és *D* transzformációk halmazának ismeretében sem képes a k_2 kulcs ismerete nélkül az *y* rejtett szövegből az *x* nyílt szöveg meghatározására. **B** az *y* rejtett üzenetből az $E_{(k_1)}(.)$ transzformáció inverzével a $D_{(k_2)}(.)$ *dekódoló transzformáció*val nyeri vissza (decryption) az eredeti *x* üzenetet:

$$x = D_{(k_2)}(y)$$

Ha $k_1=k_2$, akkor szimmetrikus kulcsú (más néven konvencionális vagy titkos kulcsú) rejtjelezésről beszélünk. Ekkor természetesen az **A** által használt $k=k_1=k_2$ kulcsot valamilyen védett csatornán keresztül el kell juttatni **B**-hez.

Ha $k_1 \neq k_2$, akkor aszimmetrikus kulcsú (más néven nyilvános kulcsú) rejtjelezésről beszélünk. Ekkor minden résztvevőnek 2 kulcsa van:

- k^P - *nyilvános kulcs* (public key)
- k^S - *titkos kulcs* (secret key)

A fenti példában az **A** a **B** nyilvános kulcsát használja a titkosításhoz: $k_1 = k_B^P$ és **B** a saját titkos kulcsát használja a megfejtéshez: $k_2 = k_B^S$, azaz:

$$y = E_{(k_B^P)}(x) \quad \text{és} \quad x = D_{(k_B^S)}(y)$$

A nyilvános kulcsú titkosítás résztvevői: A, B, C, … a nyilvános kulcsaikat: k_A^P, k_B^P, k_C^P, … elhelyezik egy mindenki számára olvasható nyilvános kulcstárban, míg a titkos kulcsukat (megfelelő

védelem mellett) titokban tartják. Egy adott felhasználó nyilvános kulcsának felhasználásával titkosított üzenetet csak az ő titkos kulcsával lehet megfejteni. A kapcsolat a másik irányban is igaz: a felhasználó titkos kulcsával titkosított üzenetet a nyilvános kulccsal lehet megfejteni.

Most nézzük meg, hogyan képes egy **A** felhasználó egy **B** felhasználónak titkos és hiteles üzenetet küldeni. Az **A** előbb a saját titkos kulcsával, majd a **B** nyilvános kulcsával kódolja az üzenetet. **B** előbb a saját titkos kulcsával, majd az **A** nyilvános kulcsával dekódol. Ekkor a hallgatózó támadó nem jut az információhoz, mert a rejtett üzenet **B** titkos kulcsa nélkül nem dekódolható, és **B** biztos lehet abban, hogy amennyiben az üzenet értelmes, akkor az üzenet **A**-tól jött, mert annak titkos kulcsát más nem ismeri.

A így kódol: $y = E_{(k_B^P)}(E_{(k_A^S)}(x))$

B így fejti meg:

$$D_{(k_A^P)}(D_{(k_B^S)}(y)) = D_{(k_A^P)}(D_{(k_B^S)}(E_{(k_B^P)}(E_{(k_A^S)}(x)))) = D_{(k_A^P)}(E_{(k_A^S)}(x)) = x$$

Problémák:

1. Hiteles nyilvános címtár kell.
2. A nyilvános kulcsú algoritmusok számításigénye nagy.

SSH összefoglaló

Szükséges kulcsok:

- gépenként nyilvános és titkos kulcs
- felhasználónként nyilvános és titkos kulcs

A kapcsolat felépítésének és működésének lépései:

1. Titkos csatorna létrehozása a kép gép között
2. A felhasználó azonosítása
3. Titkosított kommunikáció

Titkos csatorna létrehozása a kép gép között

Előfeltétel: A kliens programot futtató gépnek ismernie kell a szerver programot futtató gép nyilvános kulcsát!

A lényeg: kapcsolatkulcs létrehozása, amit a kapcsolat lezárásáig két fél minden további kommunikációja során szimmetrikus kulcsú titkosítás kulcsaként használ. Ezzel a kulccsal valamilyen titkos kulcsú algoritmussal (3DES, blowfish, CAST128, Arcfour) titkosítják az adatfolyamot.

Érdeklődőknek: Diffie-Hellman kulcscsere protokoll. (Valójában nem kulcs cseréről, hanem kulcs megegyezésről van szó.)

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

Sebezhetőség: Ha a kliens gépen nincs meg a szerver gép kulcsa, és a felhasználó úgy dönt, hogy elfogadja a – remélhetőleg a szerver által felajánlott – kulcsot, akkor azt kockáztatja, hogy amennyiben a kulcs a

támadótól származik, akkor nem a szerverrel, hanem a támadóval hozott létre közös kapcsolatkulcsot.

A felhasználó azonosítása

Az authentikáció a következő 3, erejében egyre gyengülő megoldás valamelyikével történik:

1. Erős azonosítás nyilvános kulcsú módszerrel
2. Jelszavas azonosítás
3. Berkeley r* (szerű megoldás) használata

Ezek közül a nyilvános kulcsú módszert a gyakorlatban is megismerjük.

A jelszavas azonosítás azért lehetséges, mert a jelszó is az első lépesben létrehozott titkos csatornán megy át. Éppen ebből származik a sebezhetőség is, ha a felhasználó a támadó által felajánlott nyilvános kulcsot fogadott el...

A Berkeley r* további fájlokkal bővül, a /etc/hosts.equiv és a $HOME/.rhosts fájlokon kívül: etc/ssh/shosts.equiv és $HOME/.shosts – ezzel bővebben nem foglalkozunk.

Titkosított kommunikáció

Amennyiben az előző két lépés hibátlan volt, akkor az említett hagyományos titkosítók valamelyikével titkosítják az ssh kliens és szerver közötti adatfolyamot.