Összefoglaló

Anonymity Enhancing Protocol (AEP)
Anonimitási szolgáltatásokat nyújtó hálózati protokoll

A hálózati kommunikáció elterjedésével elsőként a **biztonságtechnikai** funkcionalitást nyújtó protokollok és szabványok iránt jelentkezett igény, melyek olyan szolgáltatásokat tudnak nyújtani, mint bizalmasság, integritás-védelem, vagy letagadhatatlanság. Napjainkban már számos ilyen ismert, elterjedt, megbízható és mély szakmai tudás nélkül is alkalmazható protokoll áll rendelkezésre. Ezek használatának elterjedésével a legégetőbb problémák megoldása után a kommunikációval szemben új biztonsági követelmények merültek fel az "egyszerű", titkos és hiteles kommunikáción túl.

Az utóbbi időben egyre nagyobb hangsúlyt kap a **személyi és személyes adatok védelme** (*privacy*) és ennek megfelelően a kommunikáció során elérhető minél nagyobb szintű anonimitás. Ennek az új igénynek a kielégítésére csak részmegoldások léteznek. AEP célja egy olyan hálózati protokoll specifikációja, amely ötvözi a már bevált és ismert biztonságtechnikai eljárásokat, alapmegoldásokat, valamint a már meglevő anonimitási módszereket és általánosan alkalmazható külön hálózati rétegben megvalósított anonimitási szolgáltatásokat nyújt.

Számos olyan hálózati kommunikációs réteg ismert, amely biztonságtechnikai funkcionalitást nyújt. Ilyen az Internet világából ismert SSL, vagy a TLS, valamint az SSH, de hasonló a WAP-ban használt WTLS is. Ezek általában kliens-szerver kommunikációt tételeznek fel, melyek során biztosítják a PKI alapú kulcscserét, titkosítást, integritás-védelmet valamint a szerver és esetleg kliens oldali azonosítást is.

AEP tervezésénél ezen rétegek tulajdonságait tartottuk szem előtt. Követelményként fogalmazódott meg az egységes és könnyű használat mellett, hogy a protokollnak biztosítania kell a különböző anonimitási technikák cserélhetőségét.

Anonimitás biztosítására a két legjobban elterjedt módszer a vak-aláírás és az álnév. Az eredetileg David Chaum által internetes anonim fizetésre kidolgozott háromszereplős (bank, ügyfél, szolgáltató) **vak-aláírás** protokoll (DigiCash) teljes, visszakövethetetlen anonimitást biztosít. A másik alapmódszer az **álnév** (*pszeudo-identitás*), amely esetében az alany identitása védelmet élvez, de visszaélés esetén az álnév használója visszakövethető.

A protokoll specifikálásához először egy megfelelő leíró nyelvet választottunk. Ezek után ennek a leíró nyelvnek a segítségével a következő fázisban a különböző esetekben megjelenő lehetséges absztrakt kommunikációs partnerek és azok lehetséges tevékenységeit írtuk le. Végül a konkrét esetekhez tartozó hálózati kommunikációt specifikáltuk, melyhez a protokoll az XML szabvány leíró nyelvet használja.

Az így elkészült protokoll megoldási módszereket kínál az anonimitással együtt felmerülő visszaélések elleni védekezésre és azok utólagos felderítésének támogatására is. A munka során elkészült a protokoll JAVA implementációja, melyben az anonimitási funkcionalitást a protokoll a TCP/IP-t felhasználó SSH2 biztonságtechnikai réteg felett bocsátja rendelkezésre.

A protokoll **egységes, könnyen használható felületet** biztosít a különböző anonimitási módszerek megvalósításához, segítségével anonimitási szolgáltatásokat **mély szakmai tudás nélkül** lehet igénybe venni. A biztonságtechnikai protokollok mintájára **külön rétegben** helyezkedik el, valamint biztosítja az **anonimitási módszerek cserélésének, kibővítésének lehetőségét**.