# Informatikai biztonság

*buttyan@hit.bme.hu*

A Híradástechnika jelen száma négy áttekintő jellegű ismeretterjesztő cikket tartalmaz az IT biztonság különböző területeiről.

Az első cikk – *Szekeres László, Tóth Gergely: Szoftverbiztonság* – a szoftverhibákból származó biztonsági problémákkal foglalkozik. A mai szoftverek komplexitása elképesztően nagy, ezért szinte biztosan tartalmaznak programhibákat. Ezek a hibák egy rosszindulatú támadó számára gyakran olyan lehetőségeket rejtenek, amelyek segítségével a támadó könnyen visszaéléseket tud elkövetni, és akár a szoftvert futtató hoszt felett teljes uralmat át tudja venni. Éppen ezért a szoftverhibák kihasználása gyakran más támadások kezdőlépése. A cikk áttekintést ad a szoftverbiztonság mai helyzetéről: A szerzők ismertetik a probléma jelentőségét, kiterjedtségét és a benne rejlő kockázatokat, majd bemutatnak néhányat a tipikus szoftverhibákból. Ezt követően a hagyományos védekezési módszereket veszik sorra, rávilágítva e módszerek hiányosságaira, majd a szoftverfejlesztés folyamata közben alkalmazható védelmi lehetőségekről írnak. A cikk végül egy kitekintéssel és néhány kutatási irány felvázolásával zárul.

*Szentgyörgyi Attila és Szabó Géza: Bevezetés a botnetek világába* címmel a botnetek témakörébe vezeti be az olvasót. A botnet (robot network) egy támadó által vezérelt, fertőzött számítógépekből álló hálózat, melyet a támadó összehangolt támadások kivitelezésére tud felhasználni. A botnetek napjaink egyik legelterjedtebb és legveszélyesebb károkozói. Az átlagfelhasználó keveset tud a működésükről és a védekezési módszerekről, pedig az első botnet megjelenése óta sok év eltelt már. Ezért a szerzők összefoglalják a botnetek működési elvét, áttekintik a botnetek életciklusát a keletkezéstől, a támadások végrehajtásán keresztül a megszűnésükig, valamint a botnetek felfedezését szolgáló módszereket is és egy rövid jövőképpel zárják a cikket.

Harmadik cikkünk – *Fehér Gábor, Polyák Tamás, Oláh István: DRM technológiák* – szintén kurrens témával, a digitális tartalmakhoz kapcsolódó szerzői jogok védelmével foglalkozik. Az analóg világban egy rögzített mű másolása minőségromlással járt, így aki igazi minőségre vágyott, az kénytelen volt fizetni a tartalomért. Napjainkban azonban más a helyzet, hiszen a digitális másolat minősége megegyezik az eredeti mű minőségével. Szükségszerű tehát a digitális tartalom védelme az illegális másolás és terjesztés ellen, valamint a legális felhasználás lehetővé tétele a tartalomhoz kapcsolt felhasználási jogok definiálásával. Ezzel a védelemmel és jogkezeléssel foglalkozik a DRM (Digital Rights Management). A cikk célja, hogy az olvasót megismertesse a DRM technológia alapjaival és a javasolt DRM rendszerek működésével. A szerzők röviden tárgyalják a DRM alternatíváit is.

Végül negyedikként, *Gyöngyösi László és Imre Sándor: A kvantumkriptográfia infokommunikációs alkalmazásai* című írása egy jövőbe mutató témával, a kvantum-alapú kriptográfiával ismerteti meg az olvasót. Mint ismeretes, a napjainkban alkalmazott nyílvános kulcsú titkosító algoritmusok biztonsága nehéznek vélt matematikai problémákra, például a faktorizáció nehézségére épül. Egy kvantumszámítógép azonban ezeket a problémákat is hatékonyan (polinomiális lépésszámmal) oldaná meg. A kvantumszámítógépek megjelenésével tehát a jelenlegi titkosítási módszerek nagy része veszélybe kerül, így a jövőben olyan titkosítási módszereket kell találnunk, amelyek megvédenek bennünket egy kvantumszámítógéppel rendelkező támadótól is. Valójában régóta ismeretes a tökéletes rejtjelezés fogalma és algoritmusa, amit még egy kvantum-támadó sem tud feltörni, ám az is ismert, hogy a tökéletes rejtjelezéshez nagy mennyiségű véletlen kulcsbitet kell a kommunikáló feleknek megosztaniuk, ami a gyakorlatban szinte használhatatlanná teszi a tökéletes rejtjelezőt. Szerencsére éppen a kvantummechanika az, ami erre a problémára megoldást kínál a kvantum-alapú kulcscsere formájában, melynek segítségével a felek képesek megegyezni egy a tökéletes rejtjelezésre alkalmas véletlen kulcsban. A cikk szerzői a kvantum-kulcscsere elméleti alapjainak ismertetésén túl, annak gyakorlati megvalósításáról is beszámolnak és az olvasó képet formálhat arról, hogy hol tart ma ez a technológia.

E számunkban helyet kapott egy beküldött kutatási cikk is: *Bodrog Levente, Horváth Gábor, Vulkán Csaba: A TCP/HSDPA rendszer átvitelének analitikus modellje*. Ebben a szerzők a TCP-átvitelt modellezik mobil, adatforgalmat nyújtó, HSDPA környezetben, a TCP csomagvesztési valószínűsége és a körbefordulási ideje segítségével, megalkotják a HSDPA-t leíró sorbanállási hálózatot, amely tartalmazza a torlódási pontokat és protokollrétegeket, amelyek hatással vannak a vesztésre és a késleltetésre.

*Buttyán Levente*
*vendégszerkesztő*

*Szabó Csaba Attila*
*főszerkesztő*