Infokommunikációs rendszerek biztonsága

buttyan@crysys.hu
szabo@hit.bme.hu

Néhány évtizeddel ezelőtt a számítógépes rendszerek és a kommunikációs hálózatok tervezésénél a biztonság nem volt elsődleges fontosságú kritérium, mivel mind a felhasználók, mind pedig az alkalmazások száma erősen korlátos volt, és visszaélésre, támadásra alig akadt példa. Mára a helyzet gyökeresen megváltozott. A különböző infokommunikációs rendszerek a szó szoros értelmében mindenhol jelen vannak, körülvesznek bennünket, átszövik mindennapi életünket. A felhasználók száma nagyságrendekkel nőtt, egyes új alkalmazások pedig az adott rendszer tervezésénél meg sem fordultak a tervezők fejében, gondoljunk csak az Interneten keresztül banki tranzakciók lebonyolítására, vagy az SMS szolgáltatás használatára elektronikus fizetéshez. Mindez sajátos helyzetet teremtett: egyrészt megnőtt a biztonsági követelményeket is támasztó alkalmazások száma, másrészt – az elterjedtség mértékének növekedésével – megnőtt a potenciális támadók száma is; ugyanakkor az alkalmazásokat befogadó legacy rendszerek alapvetően semmilyen védelemet nem nyújtanak. Nyílvánvalónak látszik tehát, hogy a fejlődés nem folytatódhat a biztonsági problémák megnyugtató megoldása nélkül. Az elkövetkezendő évtized minden bizonnyal a biztonság évtizede lesz az infokommunikációs rendszerek kutatása, tervezése és építése területén.

Ez adja a Híradástechnika 2006. évi májusi tematikájának aktualitását is. Ez a szám 9 cikket tartalmaz, melyek az aktuálisan legfontosabbnak tartott biztonsági kérdések széles skáláját lefedik. Természetesen a teljes spektrum tárgyalása az adott keretek között nem lehetséges. A cikkek egy része ismeretterjesztő jellegű és átfogó képet igyekszik adni egy szűkebb területről, másik részük egy-egy fontos területhez kötődő új kutatási eredményről számol be.

A kéretlen reklámlevelek, a spamek sokunk életét megkeserítik. Szabó Géza és Bencsáth Boldizsár cikke bemutatja, hogyan juthatnak a spamerek e-mail címünkhöz, még akkor is, ha azt sehol nem publikáljuk. A cikk javaslatot tesz a DHA (Directory Harvest Attack) technika elleni védekezésre is, és bemutatja a szerzők által tervezett védelmi rendszer működését a gyakorlatban.

Sok laikus tesz egyenlőségjelet a hálózatbiztonság és a tűzfalak közé. A tűzfalak valóban fontos szerepet játszanak a védelem rendszerében, ám áttörésük nem lehetetlen feladat. Szabó István cikke bemutatja, hogy egy külső támadó hogyan tudja kideríteni a tűzfal által használt szűrési szabályokat, melyek megszerzése egy támadás első lépése lehet.

A vírusok és egyéb kártevő programok több évtizede keserítik már életünket, mégsem sikerült még megszabadulnunk tőlük. Sőt, a hálózatok terjedésével, a vírusok és férgek új erőre kaptak, s még gyorsabban képesek terjedni. Adamkó Péter cikke átfogó képet ad a kártékony programok elleni küzdelem mai helyzetéről és a védekezésben használható korszerű eszközökről.

A vírusok és férgek gyakran a rendszerben futó hasznos programok hibáit, hiányosságait használják ki arra, hogy átvegyék az uralmat a rendszer felett. Tóth Gergely és Hornák Zoltán cikke egy olyan módszert mutat be, amellyel tetszőleges programban azonosíthatók a biztonsági szempontból veszélyes hibák. A módszert megvalósító Flinder keretrendszer két lehetőséget biztosít a programozói hibák kiszűrésére: a forráskód alapú tesztelést és az úgynevezett black-box tesztelést (amikor a forráskód nem ismert).

A felhasználók mobilitását támogató vezeték nélküli hálózatok egyre nagyobb népszerűségnek örvendenek. A vezeték nélküli hálózatok azonban általában sebezhetőbbek, mint vezetékes társaik, ezért a biztonságos működés biztosítása még nagyobb hangsúlyt kap. Buttyán Levente és Dóra László cikke áttekintést ad az elterjedten használt WiFi technológia biztonsági kérdéseiről, s a kapcsolódó szabványosítási folyamatokról.

Sok mobil terminál (például telefon vagy PDA) számítási kapacitása korlátozott, ezért nem képes nagy számításigényű kriptográfiai algoritmusok futtatására. Szentgyörgyi Attila és Szüts Péter Lóránt e probléma megoldására tesznek javaslatot cikkükben. Megoldásuk lényege, hogy a nagy számításigényű kriptográfiai algoritmusokat nem a mobil eszközön hajtják végre, hanem egy speciális szerveren, melyet Security Proxy-nak neveznek.

Az elektronikus aláírás elméleti alapjai régóta ismertek. E technológia mégis csak az elmúlt években kezdett elterjedni hazánkban. Ennek egyik oka az, hogy a gyakorlati alkalmazás során számos probléma merül az elektronikus aláírással kapcsolatban. Berta István Zsolt cikke ezen problémákba nyújt betekintést, külön kitérve az elektronikus aláírás hazai helyzetére, többek között a közelmúltban közzétett elektronikus aláírás keretrendszerre.

Az elektronikus aláírás segítségével biztosítható az elektronikus tranzakciók hitelessége és letagadhatatlansága. Egy szolgáltató számára ezek fontos követelmények, ám a felhasználók érdekei gyakran ellentétesek. A felhasználók sokszor anonim módon szeretnék a szolgáltatásokat igénybe venni, amelynek biztosítására különböző anonymizer rendszerek jelentek meg. Szentpál Zoltán és Zömbik László cikke azt vizsgálja, hogy mennyire hatékonyak ezek a rendszerek, és bemutat néhány támadási lehetőséget.

Összefoglalva tehát e tematikus szám olyan kurrens biztonsági témákkal foglalkozik, mint a spam, a tűzfalak, a vírusok és egyéb kártékony programok, a programozói hibák és azok detektálásának lehetőségei, a WiFi hálózatok biztonsági kérdései, a PKI és a digitális aláírás gyakorlati problémái, valamint az anonim kommunikáció kérdése.

Buttyán Levente,
vendégszerkesztő

Szabó Csaba Attila,
főszerkesztő