ZRÍNYI MIKLÓS
NEMZETVÉDELMI EGYETEM
Doktori Tanács

GYÁNYI SÁNDOR

Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem

című doktori (PhD) értekezésének szerzői ismertetése és
hivatalos bírálatai

Budapest
2011

ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM

GYÁNYI SÁNDOR

Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem

című doktori (PhD) értekezésének szerzői ismertetése és
hivatalos bírálatai

Témavezető:

Prof. Dr. Kovács László mk. alezredes

Budapest
2011

A tudományos probléma megfogalmazása

A nyilvános adatátviteli hálózatra kapcsolódó kiszolgáló számítógépek üzemeltetése során sokszor tapasztalhatók olyan, elsőre megmagyarázhatatlannak tűnő jelenségek, rendellenességek, amelyek a gépek működésének lelassulását, időnként pedig működésképtelenségét okozzák. A hibajelenségek vizsgálata során az eszközök meghibásodására visszavezethető problémák mellett egyre többször nyer bizonyítást, hogy ezek szándékos, a rendszer túlterhelésére irányuló, úgynevezett DoS (Denial of Service) támadások. Ilyen esetekben a védekezés első lépése mindig a támadási módszer felismerése, mivel ez alapján lehetséges a védelmi eljárás kiválasztása. A védelmi eljárások egy DoS vagy DDoS támadás esetén többnyire a működőképesség minimális színvonalon történő fenntartására irányulnak egészen addig, amíg az akcióban részt vevő végpontok semlegesítése megtörténik, vagy pedig az esemény előidézője magától befejezi tevékenységét. A minimális működési szint fenntartása is gondokat okozhat, mivel a legtöbb információs rendszer nem rendelkezik akkora erőforrás tartalékkal, ami a normál működési igénybevétel többszörösét is kibírná.

Kutatásaim során az információs infrastruktúrák elleni támadási módszereket vizsgáltam, és azt tapasztaltam, hogy azok egyre komplexebbé váltak. A korábban jól elkülöníthető veszélyforrások összemosódtak, ezek szintéziséből új fenyegetések jöttek létre, amelyeket előszeretettel használnak számítógépes bűnözők és különböző politikai célú szervezetek is. A lehallgatásra vagy a célpont feletti uralom átvételére irányuló tevékenységek mellett előtérbe kerültek azok a módszerek, amelyek a célpont működésének ellehetetlenítését okozzák. Ezekre a módszerekre nincsenek általános érvényű védelmi szabályok, az újabb keletű DDoS (Distributed Denial of Service) akciókban pedig annyira sok számítógépes végpont jelenik meg támadóként, hogy ellenük nem alkalmazható a korábban bevált számítógépes hálózati adatszűrés. Egy másik, általánosan használt eljárásban a célpont igyekszik annyi erőforrást mozgósítani, amivel képes felülmúlni a támadó rendelkezésére álló kapacitást, és így „túlélni” az akciót, ennek kivitelezhetősége és főként gazdaságossága azonban kételyeket ébresztett bennem.

A legkézenfekvőbbnek tűnő megoldás az, ha a DDoS támadások elindítóját azonosítják, és vele állíttatják le az akciót. Ez könnyű feladat lenne, ha a saját eszközeit használná fel, azonban a számítógépes hálózatok természetét kihasználva ezt – érthető okból – próbálják elkerülni. A vírusok és más kártékony programok fejlesztői olyan megoldásokat szolgáltatnak, amikkel megnehezítik a tényleges elkövető személyének felderítését. A korszerű számítógépes kártevők már rendelkeznek olyan funkciókkal is, amelyek segítségével a fertőzött számítógép – vagy egyéb eszköz, amely célszámítógépet tartalmaz, és számítógépes hálózatra kapcsolódik – képes feladatokat fogadni egy központi irányító személytől. Ezek a berendezések hálózatba szerveződnek, és az így kialakult, úgynevezett botnetek kiválóan alkalmasak a túlterheléses támadások kivitelezésére. Egy botnet nagyon sok elemből állhat, ezért a semlegesítése nem könnyű feladat, főként, ha egy ilyen támadás már folyamatban is van. Nagyon fontos feladatnak tekintem ezek felderítését a tényleges támadás megkezdése előtt, amikor az időtényező még nem annyira kritikus.

Kutatási célkitűzések

Célul tűztem ki a különböző túlterheléses támadások elleni védelmi módszerek, illetve az ilyen akciók kivitelezésére alkalmas eszközök elleni ellentevékenységek kutatását.
Ennek elérése érdekében az alábbi részfeladatokat tűztem ki magam elé:

1. Megvizsgálni a különböző típusú informatikai támadási módszereket, azok veszélyeit és az általuk okozható károkat, az informatikai támadások és a hadviselés, terrorizmus kapcsolatát.
2. Felmérni a túlterheléses támadások hatásait, a velük szemben alkalmazható védelmi módszereket, a szolgáltatások fenntartását biztosító eljárásokat és ezek hatékonyságát a védelmi intézkedések megvalósíthatósága és az igénybe vett erőforrások nagysága alapján. A minél gyorsabb felismerés és azonosítás érdekében felkutatni és kategorizálni az interneten működő informatikai infrastruktúrák ellen kivitelezhető DoS és DDoS támadási módszereket, és működési elvüket.
3. Megvizsgálni a botnetek egyéb funkcióit abból a szempontból, hogy a működésük során milyen nyomok keletkezhetnek, amelyek az ilyen hálózatokat alkotó, fertőzött végpontokhoz vezetnek.
4. Olyan, a túlterheléses támadásra alkalmas számítógép-hálózati végpontok felderítésére alkalmas eljárást keresni, amely során biztosítható, hogy a végpontok tulajdonosainak személyiségi és adatvédelmi jogai ne csorbuljanak.
5. Meghatározni egy olyan rendszer alapvető funkcióit, amely segítségével a DDoS támadásokért felelős végpontok még a tényleges támadás megkezdése előtt semlegesíthetők. Megvizsgálni annak lehetőségét, hogy ez a rendszer milyen szervezeti keretek között működhetne.

Kutatási módszerek

Széleskörű irodalomkutatást folytattam az elérhető hazai- és nemzetközi irodalomban. A kutatás – témám természete és a technológia gyors változásai miatt – nagyobb részben az elektronikus, kisebb részben a nyomtatott szakirodalmat érintette. A forrásanyagok rendszerezésével és feldolgozásával bővítettem a kutatási céljaim eléréséhez szükséges szaktudásomat. Minden olyan esetben, amely során erre lehetőség volt, saját gyakorlati teszteket és számítógép-hálózati kísérleteket végeztem, amelyek eredményeivel igazoltam felállított elméleteimet.

Rendszeresen részt vettem – mind hallgatóként, mind előadóként – szakmai konferenciákon, kutatásaim eredményét rendszeresen publikáltam szakmai folyóiratokban. Munkahelyemen több olyan kutatás-fejlesztési projektben működtem közre, amely segítette szakmai fejlődésemet.

Az értekezés szerkezete

Értekezésemet négy fejezetre bontottam:

Az első fejezetben bemutatom az informatikai infrastruktúrák elleni támadások módszereit, kategóriáit, különös tekintettel a kritikus infrastruktúrák sebezhetőségeire. Elemzem az ilyen akciók katonai vonatkozásait, a hazai és nemzetközi incidenskezelés folyamatait. Egy elképzelt komplex támadás példáján keresztül bemutatom egy hazánk elleni akció lehetséges lefolyását, következményeit.

A második fejezetben bemutatom az informatikai támadások, elsősorban az úgynevezett DDoS támadások károkozó képességét, illetve az ilyen akciók elleni védekezés lehetőségeit. Kategorizálom a túlterheléses támadásokat az alkalmazott módszer és a megtámadott egység szempontjából. A szakirodalomban fellelhető gyakoribb módszereket besorolom a definiált kategóriákba, így megkönnyítve az alkalmazható védekezési lehetőségek kiválasztását.

A harmadik fejezetben elemzem a botnetek működésével, terjedésükkel kapcsolatos információkat. Ismertetem a fejlődéstörténetüket, valós és lehetséges felhasználási területeiket a számítógépes bűnözők, terroristák és katonai szervezetek szempontjából.

A negyedik fejezetben rámutatok arra, hogy egy bekövetkezett DDoS támadás során elkerülhetetlen működéskiesések lépnek fel, így fontos a megelőző tevékenység folytatása. Bemutatom egy saját kísérletem eredményét, amely segítségével a botnetek fertőzött tagjai egyszerűen, pusztán a már meglévő adatok feldolgozásával lokalizálhatók, így könnyen semlegesíthetők.

Következtetések

Életünkben egyre nagyobb szerepet kapnak a számítógépes hálózatok, amelyek védelme alapvető fontosságú, nem csak a kritikus információs infrastruktúrák esetében, de minden egyéb területen is. A nyilvános hálózatok és az általuk összekötött hálózati végpontok együttesen egy olyan virtuális teret – kiberteret – alkotnak, amelyen már jelenleg is komoly veszélyeket jelentő tevékenység zajlik. A legelterjedtebb nyilvános számítógépes hálózatot – az internetet – bűnözők, terrorista szervezetek használják információcserére, adatok eltulajdonítására, információs infrastruktúrák működésképtelenné tételére. A katonai doktrínák változása azt jelzi, hogy a hadseregek is egyre nagyobb figyelmet szentelnek a kibertérnek, ez pedig egy információs infrastruktúrák elleni, tisztán számítógép-hálózati eszközökkel előidézett konfliktus veszélyességét is megnöveli. Egy kibertérben kezdődő konfliktus eszkalálódhat, és akár államok közti fegyveres akcióvá is alakulhat.

Megjelentek az olyan számítógépes kártevők, amelyek már nem csak informatikai eszközöket veszélyeztetnek, hanem más kritikus infrastruktúrában is képes anyagi károkat okozni, emellett létrejöttek olyan nagyméretű hálózatok, amelyek összehangolt akciókra is képesek. **Megvizsgáltam korábbi kibertámadások statisztikáit, és megállapítottam, hogy az ismertté vált akciók mintegy 22%-át egy speciális módszerrel, a túlterheléses DoS támadások képezték.** A DDoS, és különösen a reflektív DDoS támadási módszerek rendkívül hatásosak, több olyan nagyléptékű esemény is történt, amelyek során a támadások több héten keresztül tartottak, így a szolgáltatás kieséséből származó veszteség is jelentős volt. Megtörtént DDoS támadások elemzésével arra a következtetésre jutottam, hogy az ilyen típusú akciók elleni védekezés első lépéseként a megtámadottnak fel kell ismernie azt a tényt, hogy támadás alatt áll. Ehhez fontos a támadási módszerek és azok sajátosságainak ismerete, ezért **felállítottam egy átlátható keretrendszert, majd irodalomkutatás segítségével összegyűjtöttem a leggyakrabban használt eljárásokat**. Az eljárásokat három fő csoportba soroltam:

- DoS támadások.
- DDoS támadások.
- Reflektív DDoS támadások.

A legnagyobb támadó potenciállal a reflektív DDoS támadások rendelkeznek, amelyek közül a DNS kiszolgálókat felhasználó módszer ellen a legnehezebb védekezni.

A támadási módszerek kategorizálására javasoltam az ISO OSI referenciamodell egyes rétegeit, aszerint, hogy a támadó a célpont melyik rétegében működő folyamatok túlterhelésére törekszik.

A védelmi módszerek elemzése azt bizonyítja, hogy a DDoS támadás ideje alatt az áldozat rendszerének működőképességét fenntartani – vagyis megelőzni a szolgáltatás kiesését – ésszerű erőforrás-gazdálkodás segítségével nem lehetséges. Mivel egy ilyen incidens során a célpont erőforrásai (számítási kapacitás, hálózati sávszélesség) és a támadók erőforrásainak összessége ütközik egymással, ezért a védelemnek előre fel kellene készülnie

az ismeretlen nagyságú kapacitást használó támadásra. A támadónak ezzel szemben a célpont meglévő kapacitásaira kell csak méreteznie az erőforrásokat, ráadásul az akciót kivitelező hálózati végpontok akár menet közben is bővíthetők újabb tagokkal, így egyszerűen növelhető a támadás intenzitása. Az informatikai rendszereket általában a normál üzemi működésre méretezik, ésszerű tartalékok biztosításával. Semmilyen szempontból nem tekinthető gazdaságosnak a normál működés sokszorosára méretezni a rendszer kapacitását, ráadásul az sem biztos, hogy ez elegendő a rendszer működésének fenntartására extrém nagy terhelés mellett.

Egy másik, elterjedt védelmi módszer a támadáshoz használt adatfolyamok tipizálása után, ezek kiszűrésén alapszik, vagyis igyekszik meggátolni a támadó által generált adatok célponthoz történő eljutását. **A DDoS és reflektív DDoS technikák vizsgálata alapján megállapítottam, hogy léteznek olyan technikák, amelyek ellen a hálózati forgalom szűrése nem kivitelezhető, mivel ez az informatikai rendszerek üzemszerű működését is gátolnák.**

Mindezek alapján bizonyítottnak látom, hogy a DDoS támadások elleni védekezés tisztán passzív eszközökkel – erőforrás növelés illetve adatfolyam szűrés – **nem vitelezhető ki ésszerű erőforrás felhasználás mellett**, ezért a támadó végpontok semlegesítését tekintem a leghatásosabb megoldásnak. A reaktív – tehát a támadást megszüntetni igyekvő – védelmi módszerek jelenleg is használatosak, és a hálózati szolgáltatók nemzetközi együttműködésén alapszanak. Bár a módszer hatásos, de ebben az esetben a problémát az időtényező okozza. Nagyszámú támadó végpont esetén sok időbe telik ezek azonosítása, majd a kiinduló hálózat tulajdonosának közreműködésével történő semlegesítése. Egy megindult támadás esetén ez az idő a célpont kiesésének időtartamát, így a bekövetkező károkat is növeli. Emiatt olyan módszerek kutatására összpontosítottam, amely segítségével a DDoS akciók potenciális eszközeit még egy támadás megindulása előtt lehet felkutatni, és semlegesíteni.

A DDoS támadások veszélyességének illusztrálására elkészítettem egy képzeletbeli, kizárólag a kibertérben végrehajtott komplex informatikai támadás forgatókönyvét. Központi elemeként a kritikus információs infrastruktúrák, vagyis az energiaellátás és a telekommunikáció elleni akciókat jelöltem meg. Veszélyes folyamatként értékeltem a mobil kommunikációs eszközök, elsősorban a mobiltelefonok informatikai biztonságának hiányosságait.

A DDoS támadások vizsgálatával megállapítottam, hogy az ilyen jellegű támadásokért leginkább számítógépes kártevőkkel fertőzött gépekből kialakított, központi felügyelet alatt álló hálózatok, úgynevezett botnetek felelősek. A botnetek vezérlési (Command & Control) csatornáinak kommunikációs módszere szerint elkülöníthető architektúrák vizsgálatával arra következtetésre jutottam, hogy vannak létező eljárások a felderítésre. Azonban ezek sokszor a felhasználók adatforgalmának figyelésével és emiatt személyiségi jogaik sérülésével járhatnak, ráadásul a számítógépes hálózatokba telepített speciális eszközök használatát teszik szükségessé. Feltételeztem, hogy a botnetek tevékenysége nem csak a DDoS támadások kivitelezésére terjed ki, ezért megvizsgáltam az egyéb irányú felhasználásukat is. **Igazoltam, hogy ezek működése olyan nyomokat is hagy, amelynek vizsgálatával meghatározhatók a kliensek elérhetőségi paraméterei**, így megnyílik a lehetőség a semlegesítésükre. Kutatómunkám során arra a következtetésre jutottam, hogy az adatlopások, különböző személyiség eltulajdonítási módszerek mellett a leggyakoribb felhasználási területük a kéretlen reklámlevél (népszerű nevén SPAM) nagy mennyiségű küldése. A botnetek tulajdonosai ebből a tevékenységből tudnak a legbiztosabban bevételhez jutni, aminek eredményeképpen az internet forgalmának jelentős hányadát ezek teszik ki, ezért véleményem szerint a legegyszerűbben felhasználható módszer a kéretlen levelek küldésére specializálódott botnetek nyomainak vizsgálata.

Az elektronikus levelezés által használt TCP protokoll vizsgálata után megállapítottam, hogy a botnetek által egyébként előszeretettel használt címhamisítási eljárások itt nem működőképesek, ezért a levelező rendszerekből kinyert adatok felhasználhatók a kliensek hálózatban elfoglalt valós helyének azonosítására. A kéretlen levelek szűrését már nagyon sok szolgáltató végzi, aminek köszönhetően a kéretlennek bizonyult levelek feladóinak hálózati címe folyamatosan rendelkezésre áll, azok megszerzésére nem szükséges külön hálózati vagy egyéb informatikai eszközöket telepíteni. A kéretlen levelek küldői között elsöprő többségben vannak a botnetek tagjai, tehát egy kéretlen levél küldőjének hálózati címe egyben egy botnet tagjának hálózati címét is jelenti. Egy, a kéretlen levelek forrásainak meghatározására használható rendszer kifejlesztéséhez **kísérleti modellt alkottam, amely a levelezőszerverekben egyébként is képződő adatok vizsgálatával képes botnetek klienseinek nyomára bukkanni**. **Működőképességének bizonyítására implementáltam a modell funkcióit**, majd a számítógépes program segítségével mintegy másfél millió, valós levélszűrés segítségével készített adatot vizsgáltam át. Az így nyert listák és a helymeghatározásra alkalmas adatbázis összevetésével bizonyítottam, hogy egy kellően pontos és naprakész adatbázis segítségével akár még földrajzi elhelyezkedés is megállapítható, de véleményem szerint a leghatékonyabb módszer a végpontok hálózati szolgáltatóját azonosító adatbázissal összevetés lehet.

A kísérleti modellel nyert tapasztalatokra alapozva felvetettem egy proaktív, tehát megelőző jellegű eljárás lehetőségét. Kutatásaim során arra a következtetésre jutottam, hogy erre egy államilag koordinált, a hazai internet-szolgáltatókat érintő rendszer a legmegfelelőbb. A rendszerhez csatlakozott internet-szolgáltatók saját elektronikus levélszűrési naplóállományukból gyűjtik ki a kéretlen levelek küldőinek hálózati címét, amelyet az alapvető szűrési feladatok – ismétlődések kiszűrése – után küldenek a koordinálást végző szervezethez. Itt történik meg a naplóállományban található hálózati címek feldolgozása, melynek során elkülönítik a hazai és a külföldi tulajdonú hálózatokhoz tartozókat. A hazai szolgáltatókhoz ezután közvetlenül jut el a veszélyesnek minősített címek listája, akik ez alapján megtehetik a semlegesítéshez szükséges lépéseket. A külföldi szolgáltatók számára a külföldi együttműködő szervezeteken keresztül jut el az információ. A módszer nagymértékben automatizálható és a rendelkezésre álló adatokra támaszkodik. Az internet-szolgáltató által küldött lista anonim, csak végpont hálózati címeket tartalmaz, így adatvédelmi szempontból sem látom aggályosnak.

Új tudományos eredmények

Értekezésem új tudományos eredményeinek az alábbiakat tekintem:

1. Valós esetekben használt támadási és védelmi módszerek elemzésével **megállapítottam, hogy egy megindult DDoS támadás során csak aránytalanul sok erőforrás bevonásával lehet fenntartani** a szolgáltatás folyamatosságát, így az ilyen védelmi eljárások önmagukban nem hatékonyak.

2. **A DDoS támadások módszereire osztályba sorolást** – külön kategóriára bontást - **dolgoztam ki**, amelyek segítségével az ilyen támadások elleni védelmi intézkedések megtétele nagymértékben hatékonyabbá tehető.

3. **A** túlterheléses támadásokért felelős **botnetek működésének elemzése után megalkottam ezek tagjainak passzív adatgyűjtési technika segítségével működő felderítési módszerét**.

4. **Kísérleti modellt alkottam** a botnet kliensek tevékenységének – kéretlen levelek küldésének nyomai – elemzésére, és helyük meghatározására, majd a megalkotott kísérleti modellel **bizonyítottam**, hogy **lehetséges proaktív módon felderíteni és semlegesíteni a DDoS támadásra használható végpontokat** (SPAM küldő végpontok) anélkül, hogy személyiségi és adatvédelmi jogokat sértenénk.

5. **Egy** olyan megvalósítható **rendszer alapjait dolgoztam ki, amely** az ismertetett eljárás segítségével **azonosítja a botnet klienseket**, majd az internet-szolgáltatók bevonásával **semlegesíti azokat**.

Ajánlások, az értekezés gyakorlati felhasználhatósága

Munkám során igyekeztem kellő alapossággal körüljárni a kibertérben előforduló veszélyforrásokat, azon belül is a DDoS támadások és az ezeket megvalósítani képes botnetek problémáját. Értekezésem egészét javaslom felhasználni a felsőoktatásban, a számítógép-hálózati támadásokkal kapcsolatos tantárgyak keretében.

Az értekezésemben szereplő kategorizált DDoS támadási módszerek segítséget nyújthatnak az ilyen támadások felismerési idejének csökkentésére, a gyorsabb és a támadáshoz leginkább illeszkedő védelmi módszer kiválasztáshoz, ezért szakmai továbbképzések kiegészítő anyagaként is felhasználható.

Az általam javasolt proaktív védelmi módszer kiépítésekor felhasználható alap irodalomként.

Saját publikációk jegyzéke

Lektorált folyóiratban megjelent cikkek

[1] DDoS támadások és az ellenük való védekezés
(Hadmérnök, 2008. február, különszám)
http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/gyanyi_rw7.html
ISSN 1788-1919

[2] Cyber-támadások elleni védekezés és a válaszcsapások lehetőségei
(Hadmérnök III. évfolyam, 2. szám, 2008. június 114-128p)
ISSN 1788-1919

[3] Botnetek felkutatása a térinformatika segítségével
(Hadmérnök IV. évfolyam 3. szám, 2009. szeptember 248-257p)
ISSN 1788-1919

[4] Elektronikus hadviselés a civil világban 1.
(Biztonság, 2008/5 36-38p)
ISSN 0864-9189

[5] Elektronikus hadviselés a civil világban 2.
(Biztonság, 2008/6 36-40p)
ISSN 0864-9189

[6] Informatikai WLAN-hálózatok zavarása
(Bolyai Szemle, 2009. április, 119-132p)

Idegen nyelvű kiadványban megjelent cikkek

[7] Next Generation Viruses
28th International Conference June 3-4, 2010.
Sience in Practice kiadvány, Subotica, Serbia

Konferencia kiadványban megjelent előadás

[8] Az információs terrorizmus fegyverei és módszerei
(Biztonságtechnikai szimpózium kiadványa, ISBN 978-963-7154-68-3, 2007. november)

Szakmai tudományos önéletrajz

Név: Gyányi Sándor

Születési idő: 1969. január 9.

Iskolák, végzettség:

Doktori Iskola ZMNE (2007 -)

Műszaki informatikus MSC, Miskolci Egyetem (2007)

Okleveles villamos üzemmérnök, Kandó Kálmán Villamosipari Műszaki Főiskola (1990)

RTV műszerész, Pataky István Híradásipari Szakközépiskola (1987)

Munkahelyek:

Óbudai Egyetem, tanársegéd (2010 -)

Budapesti Műszaki Főiskola, műszaki oktató, tanársegéd, (2003 - 2009)

Aspect Kft, üzletvezető (2001 - 2002)

Mixim Kft, üzletvezető (1991 - 2001)

Matrix Kft, vezető tanúsító (2002-2005)

Veritan Kft, vezető tanúsító (2006-)

Nyelvtudás:

Angol, általános középfokú (B2) komplex (C)

Oklevél száma: CA060-26933 876393.

Orosz, általános alapfokú (B1) komplex

Oklevél száma: EJ010-76511 1179648

Szakmai tevékenység:

1. Oktatás (Informatika II; Infokommunikációs hálózatok; Híradástechnika III;

Digitális rendszerek; Informatikai rendszerek üzemeltetése és biztonsága II. tantárgyak)

3. Kutatás-fejlesztés, szakértői munka:

Vezetékes próbahívó berendezés fejlesztése;

GTS távközlési szolgáltatások számlázásának pontossága (tanúsítás, Veritan Kft);

Pantel-Technocom SLA elszámolási rendszer fejlesztése;

Pantel-Technocom hívásadat-gyűjtő rendszer fejlesztése;

Fővárosi Gázművek elektronikus gázfogyasztásmérő adatgyűjtő rendszer fejlesztése;

Matáv RT számlázás pontosság és zártság tanúsítás (Matrix Kft);

Pannon GSM számlázás pontosság és zártság tanúsítás (Matrix Kft);

T-Mobile számlázás pontosság és zártság tanúsítás (Matrix Kft);

Emitel számlázás pontosság és zártság tanúsítás (Matrix Kft);

E-szignó elektronikus aláírás-létrehozó rendszer tanúsítás (Matrix Kft);

Kutatási területek:

Számítógépes hálózatok biztonsága

DDoS támadások

Botnetek felderítése

Digitális jelfeldolgozás