# Email-forgalomhoz kötődő gyanúgenerálási folyamatok

Pitlik László és a SZIE érdeklődő Hallgatói – 1. részjelentés

## Bevezetés

Egy virtuális cég alapításával kezdetét vette a Hallgatói probléma-érzékenység tesztelése 2012 őszén (<https://miau.gau.hu/mediawiki/index.php/INNO-WAR>). Ennek egyik rétege az email-forgalomhoz kötődő potenciális gyanúk felismerésének és az elemzéshez szükséges (létező és elképzelhető) adatvagyonok beazonosításának kérdésköre volt.

Az első gyanúmomentum keretfeltételek figyelembe vételével a relatíve lassú (vö. Pató Pál) és a relatíve gyors válaszadók felismerni tudása volt.

## 1. esettanulmány: Patópál-Detektor

### Adatvagyon-feltárás

Az adatvagyon feltárása gondolatkísérletek keretében történt, elsődlegesen nem figyelve arra, vajon egy-egy elképzelt értékelési szempont (attribútum) ma, az ismert technológiai környezetben ténylegesen naplózódik-e, ill. naplózható-e egyáltalán.

#### Módszertani kérdések

A gondolatkísérletek lényege, hogy bárki, bármilyen aspektust felvethet, melyből a többiek ki kell, hogy tudják szűrni azon jelenségeket, melyek mérhetőnek, naplózhatónak tűnnek ÉS melyre vonatozó irányokat meg lehet határozni egy-egy konkrét gyanúgenerálás kapcsán.

A felismerni vélt jelenség sokszínűek, ezeket érdemes valamilyen tezauruszt feltételezve logikai (fő/al)-csoportokba sorolni. Ilyen lehetséges logikai főcsoportok például:

* a kommunikációs hálózat hardveres és környezeti adottságai (pl. érvényes adatátviteli szabványok, aktív eszközök paraméterei, működésbiztonság, sávszélesség, kábelezések minősége, nem kábeles adatátvitel jellege, háttérsugárzás mértéke, hőmérséklet stabilitása, páratartalom stabilitása, küldő és fogadó domain fekete listázásának mértéke, delivery status-statisztikák, kiküldendő levél-késletetések/rendezések szabályai, levelezőlista-jellegű/tömegesen egyszerre kiküldendő levelek aránya a forgalomból)
* a kliens-számítógép hardveres és környezeti adottságai (pl. hálózati kártya paraméterei, processzorsebesség, összes memória, szabad memória, háttérsugárzás mértéke, hőmérséklet stabilitása, páratartalom stabilitása, kékhalál-jelenségek száma, túlmelegedések száma, kritikus szintre csökkenő memória-mennyiség fellépésének mértéke)
* a hálózat szoftverei (pl. ellenőrzések, hibajavítások algoritmusai, spam-szűrők, header-elemek száma, jellege, levelező listák karakterisztikái)
* a kliensgép szoftverei (pl. vírusellenőrzés módja, tűzfal jellege, frissítések gyakorisága, office-verzió-K, email-szoftvere-K, spam-szűrő-K, defragmentálások gyakorisága, codec-ek száma, jellege, formátum-konverzióra való felkészültség mértéke, vírusfertőzések száma, forrása)
* levéltárolás helye, módja, levélarchívum mérete (pl. saját gép, szervergép, is-is, egyéb, ill. mellékletek tárolásának helye, módja, pl. kézi címkézés jellege)
* levelezési szokások (pl. naponta érkező levelek átlagos száma, szórása, levelek mérete, mellékletek száma, mérete, fajtája, engedélyezett mellékletméret, mellékletformátumok tiltási szabályai)
* levelezőszerver elérésének módjai (pl. távoli gép, VPN, stb.)
* összevezetve és egyedileg kezelt email-címek száma (vö. automatikus forward)
* az email-üzenetek hatóköre (pl. címzettek, CC-k, BCC-k száma, előzmény-üzenetek száma, pörgési sebessége)
* email-body jellemzői (pl. alapüzenet hossza, helyesírási hibák száma, nyelvek száma, ékezetmentes-írásmód aránya, idézetek aránya, magyarul használt idegen szavak aránya, írásjelek pl. pont, vessző, kettőspont, zárójel, stb. száma, )
* levélstátuszok (pl. elküldés pillanatához képest a technikai érkeztetés időpontja, olvasásigazolás kérése, ennek időpontja, levélfontossági szintek alakulása)
* személyes adottságok a levél fogadójánál: a kliensgép naplóállományai alapján elvileg letapogatható, vajon milyen gyors a gépelés sebessége, mennyi a helyesírási hibák száma, milyen hajlandóság mutatkozik ezek javítására, mennyi időt tölt a levél fogadója az előzmények keresésével, milyen jellegű kereséseket végez, milyen módon tárolódnak a levél fogadó gépen a dokumentumok, vagyis milyen a könyvtárszervezés logikája,
* egyéb technológiai elemek: pl. van-e mobileszközre email-érkeztetés olvasási célra
* email-kezelés jellegzetességei: milyen jellegű nézeteket (pl. időrend szerint) milyen arányban használ az email fogadója, egy email-t hányszor nyit meg, milyen időbeli karakterisztika mellett
* Szövegbányászati statisztikák: adott téma kapcsán fontos kulcsszavak mely email-ekben fordultak elő, s ezeknek milyen a fentebb felsorolt összes attribútuma, ill. milyen diplomáciai kellékek milyen arányban szerepelnek egyes email-ekeben (pl. megszólítás, elköszönés, aláírás, részletes névjegy)
* A küldő szocio-ökonómiai státusza: háttér-adatbázis alapján a küldőt a teljes ismeretlenségtől a legkülönbözőbb jellegű és komplexitású kapcsolati rétegekig illik tudni jellemezni.
* …

#### Attribútumok és irányok

Néhány idézet a gondolatkísérletekből, melyek célja potenciális szabályokat megalapozó, mérhető jelenségek feltárása és a szabályok megfogalmazása a konkrét gyanúmomentum (vö. patópálizmus veszélye) szempontjából:

* „Az üzenet megértése: mennyire konkrét az üzenet, üzenet témájának lényegre törő jellege, szókincs (idegen szavak aránya), összevetés helyesírás ellenőrző programokkal, melyek egy adott szóhalmaztól való eltérést képesek mérni…
* Szabály: annál jobban érthető az üzenet, minél kevesebb idegen szó van benne százalékos arányban (háttérszabály: minél gyorsabb a megértés, annál gyorsabb lehet a válaszadás)…
* Minél kisebb az üzenet karakterszáma, annál érthetőbb az üzenet… (valóban igaz? nincs éppen egy fajta optimum az üzenet kifejtettsége szempontjából?)…
* Minél kisebb az üzenet karakterszáma, annál gyorsabban dolgozható fel az üzenet… (vö. előző kétely)…
* Minél érthetetlenebb az üzenet, annál nehezebb feldolgozni, azaz minél több idegen szó van egy üzenetben, annál lassabban lehet feldolgozni.
* Minél több összetett (minél több írásjel szerepel egy mondatban: pl. , ; - zárójel) mondat van egy üzenetben, annál lassabban dolgozható fel (annál nehezebben érthető).
* Technikai háttér: a küldés pillanatához képest mikor érkezett meg az üzenet egyáltalán a feladó emailbox-ába, mikor ment ki az olvasásigazolás igazolás egyáltalán…
* Az üzenet fontossága milyen szintű…
* A fogadó több e-mailcíme közül melyikre érkezett (mennyire fontos az az e-mailcím) azaz hány százalékát bonyolítja az „össz-emailforgalomnak” ezen címről”…

Minden egyes, a módszertani fejezetben jelzett potenciális szempontra pontos definíció (jelentés, naplózás mikéntje, helye) és irány megadása:

…

### Elemzések

<http://miau.gau.hu/oktatas/2012osz/reakcioido2.xlsx>

<http://miau.gau.hu/oktatas/2012osz/reakcioido.xlsx>

## 2. esettanulmány: Vírusfertőzési kockázat-detektor

Milyen email-attribútumok és irányok mentén lehet feltárni, vajon melyik küldemény megnyitása milyen mértékű kockázattal jár vírusfertőzési kockázatok szempontjából?

…

## 3. esettanulmány: Válaszadási preferencia-javaslatok

Milyen email-attribútumok és irányok mentén lehet feltárni, vajon melyik küldeményt illik megválaszolni legkorábban a még „nyitott kérdések” közül?

…

## 4. esettanulmány: Farkas-fakras!-detektor

Milyen email-attribútumok és irányok mentén lehet feltárni, vajon melyik küldemény visel indokolatlanul túl magas sürgősségi jelzést?

…

## 5. esettanulmány: Haladék-detektor

Milyen email-attribútumok és irányok mentén lehet feltárni, vajon melyik küldemény esetén milyen mértékű és formájú haladékra mikortól van szükség? (a formális és azonnali haladékkéréstől a taktikus email-hibagenerálásig: pl. egy-egy karaktersor kiemelése egy docx file fejlécéből automatikusan olvashatatlan, de megküldött válaszhoz vezet)

…

## 6. esettanulmány: Formátum-detektor

Milyen email-attribútumok és irányok mentén lehet feltárni, vajon melyik küldemény esetén illik/szabad egyes diplomáciai levélkellékektől eltekinteni, ill. milyen maximális terjedelmű választ illik küldeni (vö. idézetek aránya, mellékletek jellege pl. mobilkommunikáció esetén)

…

## 7. esettanulmány: Olvasásigazolás-detektor

Milyen email-attribútumok és irányok mentén lehet feltárni, vajon melyik küldemény esetén illik kiengedni az olvasásigazolást? (A jogszabályilag, vagyis deklarált előírások formájában létező kötelezettségek megsértésének utólagos feltárása nem ide tartozó jelenségkör.)

…

## 8. esettanulmány: …-detektor

Milyen email-attribútumok és irányok mentén lehet feltárni, vajon melyik küldemény esetén …

…

Feljegyzések:

Az email-ek szabályozása hatósági, jogi folyamatokban: rövid, anonimizált esettanulmányok arról, milyen szervezet milyen élethelyzetben miként járt el tévesen

* pl. hogyan lehet egy saját domain-t üzemeltető állami szerv „biztonsági kisegítő” mailszerver-szolgáltatása a gmail.com
* milyen szervezetek milyen publikus címlistákat tartanak fenn (pl. nav, ügyészség)
* milyen szervezetek milyen ügyfélkapus szolgáltatások kialakítása esetén tér le az email-váltásról (nfh)
* miként oldható fel a nagyméretű mellékletek eljuttatásának kérdése a címzetthez, ha az ügyfélkapus rendszer korlátai nem ismertek pontosan (nfh)
* milyen szereplők milyen módon vehetők rá az olvasásigazolás kiengedésére, ami nem más, mint a tértivevényes postai küldemény digitális megfelelője
* …

Intézményi, vállalati email-forgalom potenciális anomáliái

* szabad-e pl. a google-calenders szolgáltatásait igénybe venni hivatalos intézményi kommunikáció kapcsán
* mikortól szükségszerű átállni a kézi vezérlésről portálok által támogatott (archivált és szabályozott) kommunikációra
* …

Privát email-forgalom anomáliái

* hogyan lehet felkészülni a legelavultabb kliens-oldali megoldások (pl. weben keresztül megnyitott és semmilyen tartalmat mutatni nem akaró üzenetek) negatív hatásainak tompítására
* …

A netikett részletes értelmezése és az ebben fellelhető email-specifikus attribútumok értelmezése gyanúgenerálási szempontból: http://hu.wikipedia.org/wiki/Netikett