HunCERT Workshop

Hamis vagy valódi-e a feladó?

Dravecz Tibor, INTEGRITY Kft.
2018. november 14.

Tartalom

Honnan ered a probléma?

Az email phishing probléma alapjai:

- hamis címet adhat meg a feladó,
- költséghatékonyan, könnyen és büntetlenül lehet spammelni.

Hagyományos levelekkel is követnek el csalásokat, csak éppen relatíve költséges volta miatt ez kevésbé hatékony visszaélési mód.

Hamis vagy valódi-e a feladó?

A kérdés jóval túlmutat a phishingen - sokkal általánosabban fontos, hogy meg tudjuk állapítani, hogy

- egy levélnek ki a szerzője,
  - valóban az a szerzője, mint a levél állítja,
  - vagy más? - esetleg hamis vagy csaló levéllel van dolgunk?

Hogyan ellenőrizhetjük, hogy valóban a szerző küldte a levelet?

- Klasszikus megoldás a visszakérdezés;
- jó megoldás lehet a digitális aláírt levél,
- és vannak más megoldások, melyek több-kevesebb bizonyosságot adhatnak.

Nem triviális, hogy a levél aláírója-e a szerző, vagy a valóban felelős aláíró,

- se postai levél,
- se email esetében.

Megjegyezzük telefonhívás, fax üzenet vagy SMS üzenet esetén a hívószám kijelzés szintén lehet hamis, bár a gyakorlatban ritkább ezzel a visszaélés.

Email (és elektronikus dokumentumok) esetén azonban sokkal jobbak a verifikációs lehetőségeink, mint hagyományos levél vagy akár telefonhívás, fax vagy SMS esetén,

- gondoljunk csak a digitális aláírásra,
- de ezen túl is további lehetőségek vannak.

Megjegyezzük, hogy a digitális aláírás - legyen az akár minősített aláírás - a megtévesztések újabb tárházát adja :-(

A false negatív és false pozitív ítélet gondja

- A legrosszabb, ha hamis levelet valósnak gondolunk,
- de sok kellemetlenség adódik abból is, ha valós levelet hamisnak vélünk.
- Ugyanakkor sok kellemetlenséggel, kényelmetlenséggel, plusz munkával járhat az, ha nem tudunk könnyen dönteni arról, hogy egy levél hamis vagy valódi.

Hagyományos postai levél

Boríték

Feladó neve és címe

Címzett neve és címe

Levél

Gipsz Jakab és társai Kft.
Kukutyin, Lenin út 3.
+41 99 999-999

Piros Arany részére

Tárgy: minta

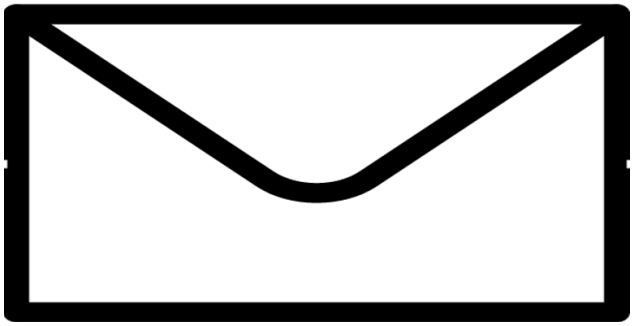
Tisztelt Piros Arany!

…

Kelt, …

'Aláírás'
név

Email üzenet



= boríték (envelope) + levél (content)
(Simple Mail Transfer Protocol /SMTP/, RFC 821/5321)

levél (content) (Internet Message Format, RFC 822/5322)

- **headers (fejléc)**
- **body**

Hagyományos postai levél versus email

POSTAI LEVÉL:	**EMAIL:**
Boríték: Feladó neve, címe + Címzett neve, címe Postahivatalok bélyegzői, jelzései	**Boríték (RFC 5321, STMP):** Return-Path: <**returnpath email address**> Delivered-To: piros@addresseedomain2 Received: from MX Received-SPF: Pass (sender SPF authorized) … **envelope-from=…** **[RFC5321.From]**; Received: from from Providerdomain (Providerdomain [ProviderIPaddress]) Received: from WORKSTATION
Levél: • **Fejléces papír** • **Levél szövege**	**Levél fejléc:** Authentication-Results: ...-DMARC; dmarc=pass header.from= senderdomain Authentication-Results: ...-DKIM; dkim=pass (2048-bit key; secure) header.d=DKIMdomain header.i=@domain ...; dkim-adsp=pass; dkim-atps=neutral DKIM-Signature: ... **From: "Gipsz Jakab" gipsz.jakab@senderdomain [RFC5322.FROM]** To: = piros.arany@addresseedomain1 Subject: test Date: Thu, 8 Nov 2018 19:03:15 +0100 Message-ID: <003d01d4778d$52a276a0$f7e763e0$@domain>

Email küldés és email üzenet

Továbbítás **Simple Mail Transport Protocol /SMTP/ (RFC 821/5321),** **mely egy host-to-host protokoll**	**Üzenetformátum** **Internet Message Format (RFC 822/5322),** **mely üzenetformátum**

Simple Mail Transport Protocol /SMTP/	RFC 821 Internet Standard, 1982 Obsoleted by: 2821	RFC 2821 Proposed Standard, 2001 Obsoleted by: 5321	RFC 5321 Draft Standard, 2008
Internet Message Format	RFC 822[1] Internet Standard, 1982 Obsoleted by: 2822	RFC 2822 Proposed Standard, 2001 Obsoleted by: 5322	RFC 5322 Draft Standard, 2008

[1] Obsoletes: RFC 733

'Teljes fejléc'

Return-Path: <**pityipalko@*sender***> [RFC5321.MailFrom]
Delivered-To: piros@*addresseedomain2*
Received: by MAILSERVER ...
    id C71E912006F; Thu, 8 Nov 2018 20:58:58 +0100 (CET)
X-Spam-...
Received: from MX (MX [IPaddress]) ...
Authentication-Results: ... dkim=pass (2048-bit key; secure) header.d=integrity.hu header.i=@*author* header.b=X3P56n1v; dkim-adsp=pass; dkim-atps=neutral
Received-SPF: Pass (sender SPF authorized) ... **envelope-from=pityipalko@*sender* [RFC5321.From]**; ...
Received: from **mailprovider** (**mailprovider** [IPaddress)
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
    (Client CN "*.**mailprovider**", Issuer "HyperTLS RSA CA 2018" (verified OK)) by MX ...
Received: from PITYIPALKO-WKS (cable-1-2-3-4.xx.internet.service.provider [1.2.3.4]) ...
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=***DKIMdomain***; s=mail; t=1541707138; bh=5g4AGpsLRnq0GuQ…=;
    h=From:To:Subject:Date;   b=X3P...
From: "Gipsz Jakab" <**gipsz.jakab@*author***> [RFC5322.From]
To: "Piros Arany" piros.arany@*addresseedomain1*
Subject: test
Date: Thu, 8 Nov 2018 20:58:57 +0100
Message-ID: <000201d4779d$7bea23e0$73be6ba0$@*domain*>
...

Kétféle 'from'

Boríték from - Envelope from (RFC 5321 MailFrom)

Levél(fejléc) from -Headers from (RFC 5322 From)

Mindkét 'from' könnyen hamisítható! - felhasználókkal ezt tudatosítani kell!

A levelező kliensek tipikusan csak a 'levélfejléc from'-ot mutatják
- bár jellemzően megnézhető a boríték from is (több-kevesebb kényelmetlenség árán).

Headers szerző/feladó/válasz címek (RFC 5322, 6854; RFC 4021):

- "From:" ("Mailbox of message author", RFC5322.From)
- "Sender:" ("Mailbox of message sender" - "Specifies the mailbox of the agent responsible for the actual transmission of the message.")
- "Reply-To:" ("Mailbox for replies to message")
- "Resent-From:" ("Mailbox of person for whom message is resent[2]")
- "Resent-Sender:" ("Mailbox of person who actually resends the message[3]")
- … (nem szabványos és elavult hasonló mezők is lehetségesek)

"Return-Path:" (reverse path, bounce address, reverse path, envelope from, Mail From, MFrom, RFC5321.MailFrom - "Message return path" - "Return path for message response diagnostics.")

[2] Contains the mailbox of the agent who has reintroduced the message into the message transfer system, or on whose behalf the message has been resent.
[3] Contains the mailbox of the agent who has reintroduced the message into the message transfer system, if this is different from the Resent-From value

Megoldás

- Tájékoztatás, képzés, ellenőrzés

- Digitális aláírás alkalmazása
  - szervezeten belüli bevezetése, rendje, menedzsmentje
    - + tájékoztatás, képzés, ellenőrzés

- Email authentikációs eljárások alkalmazása (DNSSEC + SPF + DKIM + DMARC)
  - szervezeten belüli bevezetése, rendje, menedzsmentje
    - + tájékoztatás, képzés, ellenőrzés

- *Amint elérhetők lesznek, újabb technikák bevezetése (DANE, SMIMEA stb.)*

Említett technikák

- **Elektronikus aláírás** (S/MIME - X.509, *PGP*)

- **DNSSEC** (Domain Name System Security Extensions)
  - **DANE** (DNS-based Authentication of Named Entities)

- **Email authentication**
  - **DKIM** (DomainKeys Identified Mail)
  - **SPF** (Sender Policy Framework)
  - **DMARC** (Domain-based Message Authentication, Reporting and Conformance)
  - …
- DANE + PGP, DANE SMIME

- **rDNS** (Reverse DNS lookup)
  - (FCrDNS - Forward-confirmed reverse DNS)

- **MTA-to-MTA közötti TLS kommunikáció**
  - DANE SMTP

Mindezen technológiáknak vannak gyengeségei!

Mindenezen technilógiákat lehet rosszul alkalmazni vagy használni!

Nincs 100 %-os megoldás! - mindezen technológiák együtt sem adnak 100 %-os megoldást.

Ne azt várjuk, hogy a spamek számát csökkentik ezen technikák alkalmazása! - ha irreálisak az elvárásaink, akkor csalódnunk kell.

SPF, DKIM, DMARC együtt igazán hasznos, külön-külön csekély értékűek!

Sok-sok negatív kritikával szemben állítjuk, hogy ezek mindegyike jó technika[4], ha megfelelően alkalmazzuk őket.

[4] a lehetőségekhez képest jó megoldások

Miért nem elég a digitalis aláírás?

Elektronikus aláírás előnyei és hátrányai

Hátrányok:

1. **Aláírás generálás és ellenőrzés, valamint kommunikációs és tár overhead.**
2. **Lejárt vagy visszavont tanúsítványok esete.**

Továbbá:

- A privát kulcskezelésnek is van overheadje és biztonsági kockázata. Alkalmazásának is van overheadje.
- CA tanúsítványok elfogadásának kérdése.
- Invalidként megjelölt üzenet nem feltétlenül hamisat jelent.
- Nem aláírt üzeneteket indokolatlanul érvénytelennek (invalid) tekinthetnek.
- Bizonyos eszközök nem támogatják.
- Aláírás is lehet hamis vagy helytelen; tanúsítvány is lehet nem megfelelő, vagy nem kielégítő.
- Minimális szakértelmet a használata - különösen a helyes és értelmes használata - is igényel, mind küldő, de még inkább fogadó oldalon (pl. észre kell tudni venni, hogy akár egy érvényesnek minősített aláírás adott esetben nem hitelesíti vagy nem kellően hitelesíti a küldőt).
- Plusz költség (bár tanúsítvány ingyenesen is elérhető, sőt lásd: DANE).

Ezek egy része nem hátrány, csak esetleg éppen nem a várt előnnyel jár a digitális aláírás használata.

Kérdés: érdemes-e minden levelünket aláírni?

Fő probléma: nem eléggé elterjedt, nem elég mindannapi a használata - különösen indokolt esetekben is igen gyakran nem alkalmazzák.

Miért kell a digitális aláírás mellé DNSSEC+SPF+DKIM+DMARC is?

Miért kell a DNSSEC+SPF+DKIM+DMARC mellé digitalis aláírás is?

Mindkettő más szintet képvisel, a digitális aláírás az email üzenetet (vagy az email üzenetben küldött dokumentumot) hitelesíti, annak feladóját és teljes tartalmát,

míg kissé leegyszerűsítve az MTA TLS, DNSSEC, SPF, DKIM, illetve DMARC a küldő szervereket, domaineket, illetve küldő címét hitelesíti.

Másrészt ezek egymást erősítik, mert digitális aláírás is lehet hamis (vagy helytelenül használt), vagy kétes, és ekkor az MTA TLS, DNSSEC, SPF, DKIM, DMARC megerősítésként szolgálhat vagy kételyt erősíthet meg.

Lényeges a különbség, hogy a digitalis aláírást rendszerint végfelhasználó ellenőrzi, míg az SPF-et kifejezetten a levelezőszerverek, a DNSSEC-et tipikusan resolverek, bár a végfelhasználó kliense is ellenőrizheti, és hasonló igaz a DKIM-re és DMARC-ra is.

DNSSEC, SPF, DKIM, DMARC használat

Indokolatlanul sokan nem alkalmazzák a DNSSEC-et, DKIM-et és DMARC-ot,

- sőt nagyon sokszor akkor sem alkalmazzák ezeket, amikor az igen csak elvárható lenne!
- Miért nem alkalmazza ezen eszközöket az állami hivatalok, hazai (nagy) szolgáltatók … többsége??!

Megjegyzés: Az SPF-et nagyon sok olyan domainnél nem alkalmazzák, ahol hasznos lenne alkalmazni.

Internet mail

Az Internet mailhez mintaként elsősorban a hagyományos postai levél, illetve levelezés szolgált, bár megjelenésekor már más elektronikus levelező megoldások léteztek.

Az Internet mail első szabványa 1982-ben jelent meg:

SIMPLE MAIL TRANSFER PROTOCOL (SMTP), RCF 821

mely üzenet formátumára a STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES, RFC 822 (1982) társszabvány született, mely az Internet elődjének, az Arpanetnek az üzenet küldési 1977-es RFC 733 szabványából indult ki.

Ez a két szabvány, azaz az RFC 821 és az RFC 822 határozza meg ma is alapvetően az Internet levelezést, formailag ma is az RFC 821/822 páros az Internet mail hivatalos szabványa[5], gyakorlatban pedig az Internet levelezés de facto szabványa ennek sokszoros kibővítése[6].

Miért is fontos ez? - Azért, mert az Internet levelezés alkalmazása legkevésbé a technikai alapok tekintetében változott, minden más szempontból viszont óriási volt a változás.

[5] Internet Standard
[6] gondoljunk csak például a multimédia üzenetekre

Hasonló történt a DNS tekintetében is, a protokoll megjelenését követően lényegében nem változott, csak bővült, és az örökségét azóta hordozza.

A Domain Name System (DNS) az Internet mailtől elválaszthatatlan, melynek 'szabványai' az RFC 881, 882, 883 1983-ban jelentek meg.

A spam, és email phishing elleni küzdelem alapvetően nem más, mint folyamatos toldás-foldás (patkolás). Az eredeti szabványokhoz és a világ egységes Internetes levelezéséhez, azaz az 1980-as évek eleje örökségéhez muszáj volt, muszáj ma is, valamint muszáj is lesz alkalmazkodni. Látszólag nem a legjobb megoldásokkal találkozunk, melyre ekletáns példa az SPF[7], a DKIM[8], vagy hasonlóan DNS terén a DNSSEC, de a körülményekhez képest ezek valójában nem rossz megoldások - a lényeg, hogy hasznosak és használhatók.

DNS tekintetében minden bizonnyal megjelenthetett volna egy verzió 2-es, Internet mail esetén ez sokkal nehezebb lett volna.

Akárhogy is a kihívásokra csak folyamatos toldás-foltással (patkolásokkal) lehetett csak válaszolni, ezek közül vannak egész jól sikerültek is, mint például a DMARC[9] (vagy említhetjük a DANE[10]-t, mely egy valóban briliáns megoldás).

[7] Sender Policy Framework
[8] DomainKeys Identified Mail
[9] Domain-based Message Authentication, Reporting and Conformance
[10] DNS-based Authentication of Named Entities

Az ISzT által támogatott hálózathasználati irányelvek (AUP - Acceptable Use Policy)[11]

4. Az elektronikus levelezésre vonatkozó irányelvek

4.1. Tilos a szolgáltató hálózatát vagy szervereit nagy terjedelmű vagy nagy mennyiségű levelek, illetve kéretlen kereskedelmi üzenetek (együttesen spam) küldésére használni. Ilyennek minősülhetnek többek között a kereskedelmi reklámok, tájékoztató bejelentések, karitatív kérések, aláírásgyűjtések és politikai vagy vallási röpiratok. Hasonló tartalmú üzeneteket csak akkor szabad küldeni, ha valaki ezeket kifejezetten igényli (l. elektronikus kereskedelmi törvény).

4.2. Tilos a szolgáltató hálózatát vagy szervereit kéretlen, nagy mennyiségű, illetve kereskedelmi elektronikus levelekre való válaszok begyűjtésére használni. Tilos a szolgáltató hálózatán igénybe vett, illetve az ügyfél által nyújtott bármely szolgáltatást a 4.1. pontban leírt módon reklámozni.

4.3. Tilos hamisítani, illetve megtévesztés céljából a levél fejlécét megváltoztatni vagy törölni. Mivel azonban számos vírus, féreg, illetve spam küldő ezen tilalom ellenére meghamisítja a feladó címét, ezért tilos automatikus figyelmeztetést küldeni a feladónak vagy a címzettnek a vírus, féreg, illetve spam eltávolításával, eldobásával kapcsolatban, amennyiben a feladó vagy a címzett nem a szolgáltató saját ügyfele.

4.4. Tilos számos kópiát küldeni azonos vagy nagyon hasonló levelekből. Ugyancsak tilos igen hosszú üzenetek vagy fájlok küldése egy címzettnek a levelező szerver, illetve a felhasználói hozzáférés megbénítása szándékával (mail bombing).

4.5. Tilos küldeni, illetve továbbítani "hólabda" leveleket (chain letters: üzenet, amelyben olyan felhívás van, hogy a címzett küldje tovább az üzenetet másoknak), vagy hasonló üzeneteket, függetlenül attól, hogy ezekben folyamodnak-e vagy sem pénzért, illetve egyéb értékért, valamint függetlenül attól, hogy a címzettek kívánnak-e vagy sem ilyen leveleket kapni, kivéve, ha a címzett előzetesen hozzájárult az ilyen levelek küldéséhez.

4.6. A szolgáltató hálózatát és szervereit nem szabad olyan másik Internet szolgáltatótól küldött levelekre való válaszok fogadására használni, amely levelek megsértik a szolgáltató vagy a másik Internet szolgáltató szolgáltatási irányelveit.

4.7. Amennyiben valaki egy másik Internet szolgáltató szolgáltatását veszi igénybe egy, a szolgáltatónál elhelyezett web lap reklámozására, úgy köteles olyan reklámozási technikákat alkalmazni, amelyek megfelelnek az Irányelveknek.

[11] V1.1. Utolsó módosítás:2013.04.09.

ISZT AUP frissítése

Az ISZT AUP frissítése szükséges, különösen az email authentikáció terén.

Messze nincs konszenzus.

Különösen az SFP megítélése terén eltérőek az álláspontok, azonban

- SPF terén is vannak egyértelműen kimondható javaslatok[12], ilyenre példa:
    - ha egy domainnél egyáltalán nincs levelezés, akkor "v=spf1 -all" alkalmazandó.

[12] ez sajnos nem egy kimondott, széles körben alkalmazott javaslat

Függelék:

Digitalis aláírás és tanúsítványok helytelen használata és velük való visszaélési lehetőségek

- **Nem a szerző privát kulcsával történő aláírás** (például az állami ügyfélkapu által biztosított minősített dokumentumaláírás NISZ minősített tanúsítványával).
- **Hiányos tanúsítvány** (a tanúsítvány nem elégséges az aláíró egyértelmű azonosítására)

Új lehetőségek

- **Az eSzemélyi, mint aláíró eszköz**
  - nagy előnye, hogy a tanúsítvány egyértelműen azonosítja az aláírót (a személy igazolvány számot tartalmazza)
- **Új eszközök: DANE, DANE-PGP, SMIMEA stb.**

Szerzői jogi kikötés:

Ezen anyag bárki által szabadon felhasználható (beleértve, hogy terjeszthető, továbbadható, közzétehető) egészében vagy részleteiben, mindaddig amíg a felhasználó hivatkozik a szerzői jog tulajdonosára az INTEGRITY Kft-re.