Domén- és DNS-biztonság: alapfogalmak

2020. november 19.

Dravecz Tibor, INTEGRITY Kft.

Kérdések küldhetők:
mailto:webinar2020november19@integrity.hu [1]

[1] 2020. november 25-ig él ez a cím

Three fundamental parts of the Internet infrastructure:

Border Gateway Protocol (BGP)

helps exchange routing information over the Internet

Domain Name System (DNS)

is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet

Network Time Protocol (NTP)

is the de-facto means Internet hosts use to synchronize their clocks

DOMAIN NAME SYSTEM

- Internet (Internet ≠ internet)

- doménnév
- doménnévtér
  - Internet doménnévtér
- domén
- Domain Name System (DNS)
  - Internet Domain Name System (DNS)

- DNS zóna
- DNS rekordok

TTL, rekordtípusok, névszerver, authoritatív névszerver, névfeloldás, DNSSEC …, doménnyilvántartó, -regisztrátor, -igénylő, -használó, regisztráció, -fenntartás, …

Doménnév (domain name) és -névtér

Internet doménnévtér (Internet domain name space)[2]

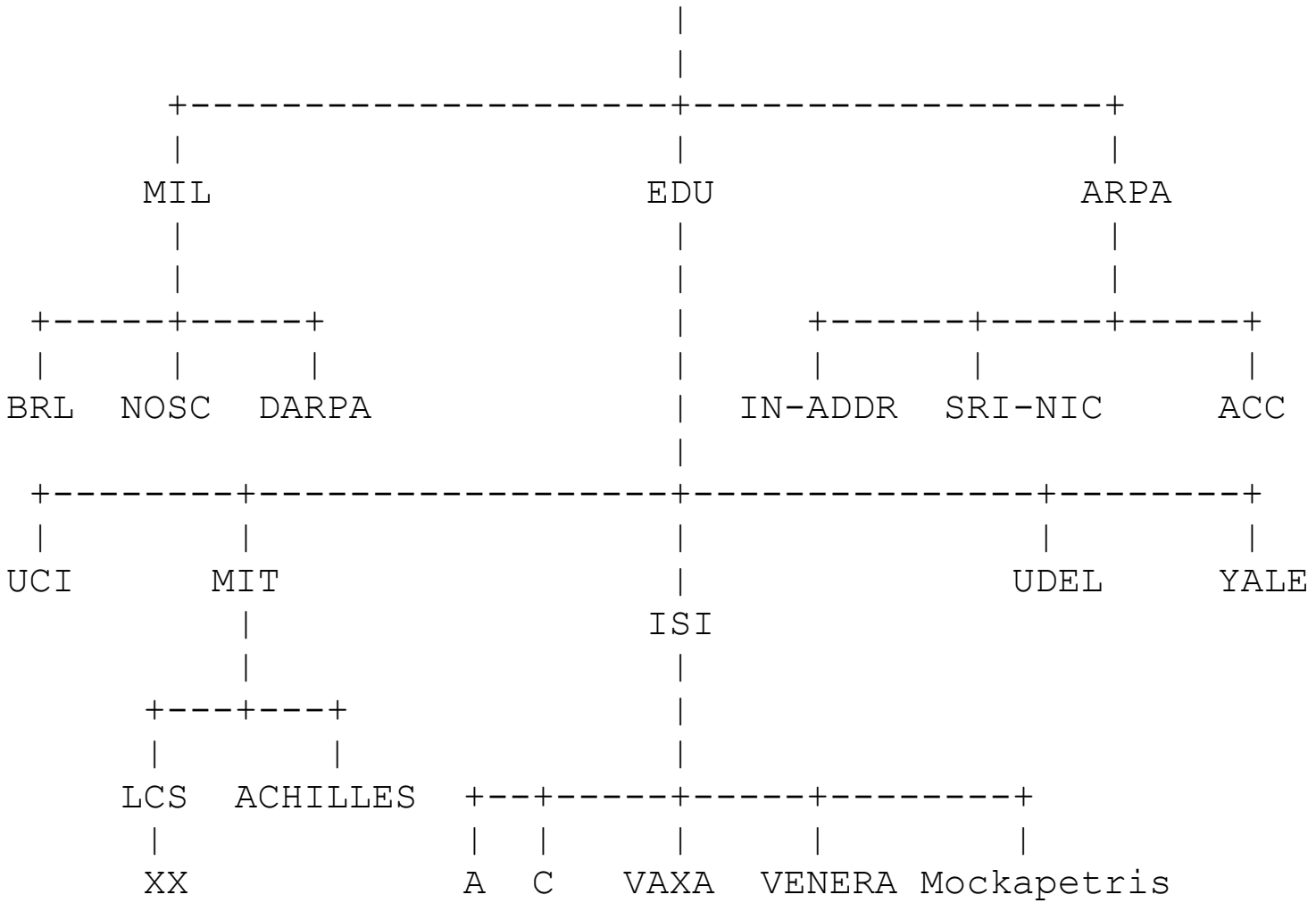
A doménnév tér egy fastruktúra,

- mely node-okból áll,
- minden node-ot egy és csak **címke (label)** jelöl,
  - címke 0-63 oktettből áll,
  - a zéró hossz, melyet ’null’-nak nevezünk fenntartott a fa gyökerének (root).

null — **root** (.)
|
node — **top level domain** (hu.)
|
node — **second level domain** (domen.hu.)
…
|
node

[2] https://tools.ietf.org/html/rfc1034

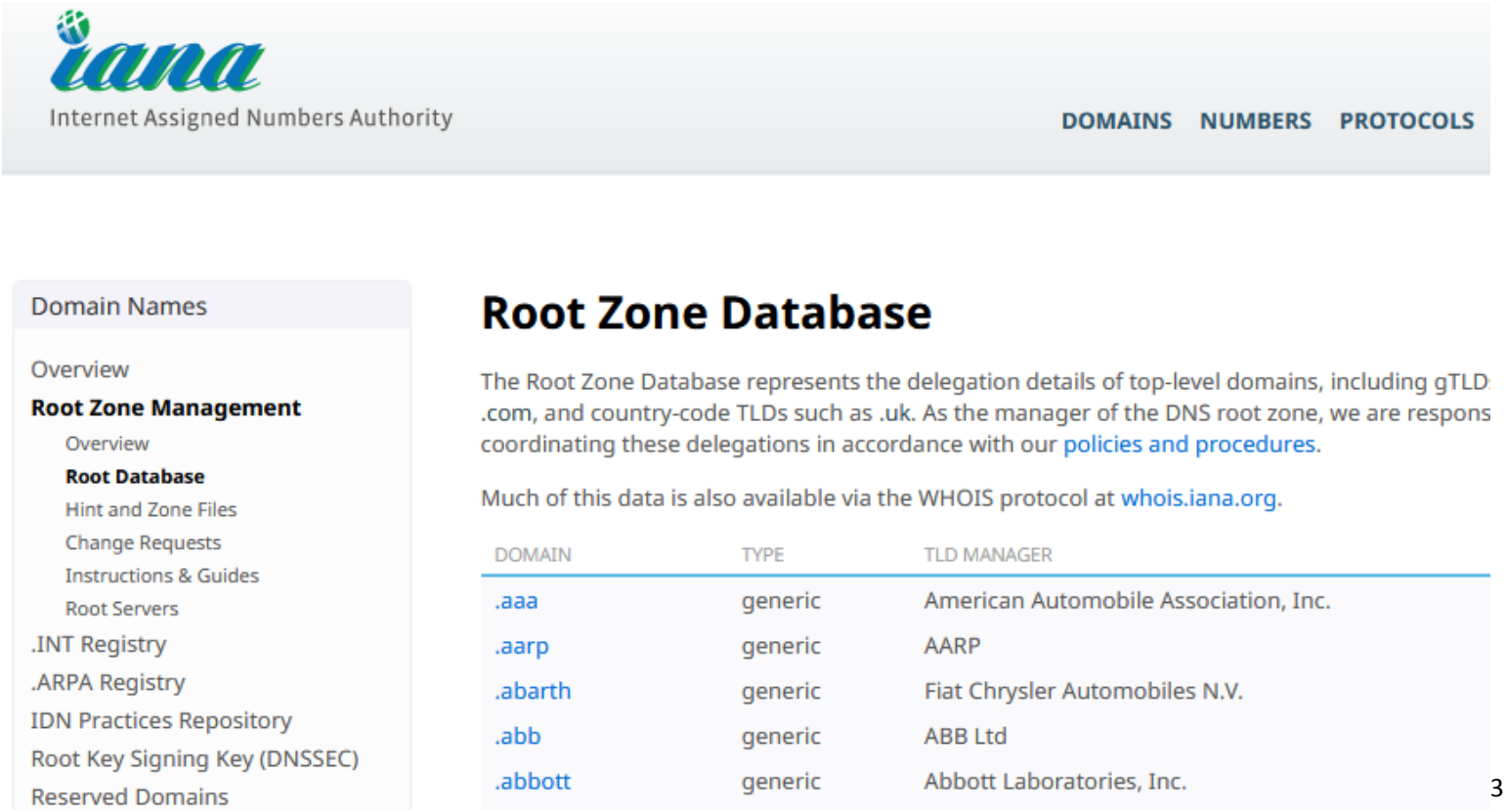
A mai webinárunk során a következőkben csak **az ember által olvasható írásos reprezentáció**ját fogjuk használni.



https://tools.ietf.org/html/rfc1034

A címkék **case-insensitive ASCII karaktertek**ből állnak (de az alkalmazásoknak szabvány szerint meg kellene őrizniük a kis- és nagybetűket).

Felső szintű domének (TLDs)



[3]

[3] https://www.iana.org/domains/root/db

Erőforrás-rekordok (resource record /RR/)

A doménnévtérben az egyes node-okhoz **erőforrás-halmazok (resource set)** tartoznak, melyek lehetnek üresek is.

www.domen.hu	doménnév és **hosztnév**
domen.hu	doménnév és hosztnév
hu	doménnév
. (root)	doménnév

LABEL	TYPE	IN	TTL	RESOURCE
www.domen.hu.	A	IN	300	212.52.164.124
domen.hu.	A	IN	300	212.52.164.124
test domen.hu.	A	IN	30	212.52.164.124
test2.domen.hu.	CNAME	IN	900	test.domen.hu.
domen.hu.	MX	IN	3600	mx1.anonymail.hu. 10
domen.hu.	MX	IN	3600	mx2.anonymail.hu. 10
au domen.hu.	MX	IN	1800	a.mx.integrity.hu

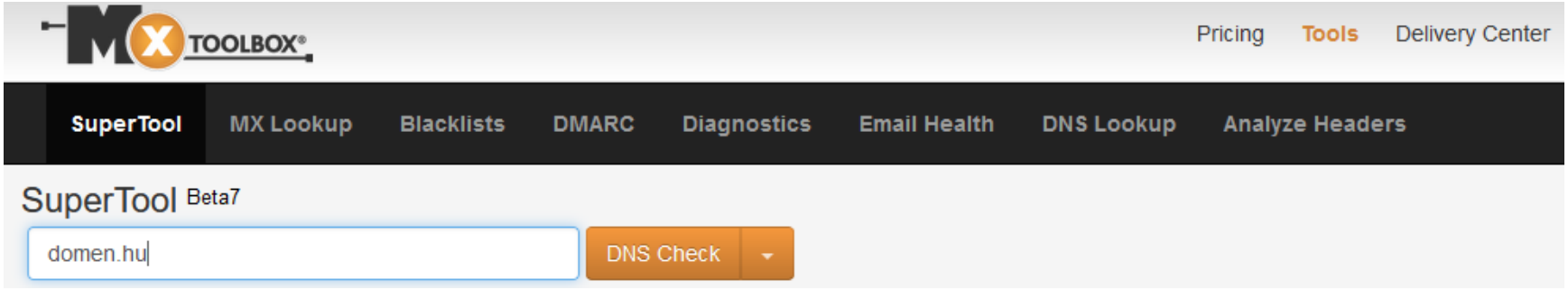
DNS zóna fogalma

Eszközök (tools)

Parancssoros eszközök:

nslookup (csak a teljesség kedvéért említjük)
dig (BIND, Linux, Windows)
resolve-dnsname (PowerShell /hiányos, befejezetlenül hagyta a Microsoft a fejlesztését/)

Online (webes) eszközök:



https://mxtoolbox.com

ICANN

Registries (nyilvántartók)

Registrars (regisztrátorok)

Resellers (viszonteladók)

Clients (előfizetők)

Registrants (‘tulajdonosok’)

tényleges doménhasználók

felhasználók

más érintettek/érdekeltek

- szabályozás,
- szabályozó testületek
- jogalkotás
- vitarendezés
- igazságszolgáltatás
- hatóságok

Doménregisztráció és DNS-szolgáltatás

Doménregisztráció

- doménigénylés
- doménfenntartás

Authoritatív névszerver-szolgáltatás

Egyik leginkább kiszervezett szolgáltatás: a DNS-szolgáltatás.

Névfeloldás

>dig **domen.hu** +trace +noall
;; Received 525 bytes from 1.1.1.1#53(**1.1.1.1 - RESOLVER**) in 15 ms

;; Received 801 bytes from 193.0.14.129#53(**k.root-servers.net - ROOT**) in 15 ms

;; Received 544 bytes from 193.239.148.1#53(**a.hu - TLD ROOT**) in 6 ms

;; Received 221 bytes from 176.97.158.100#53(**sec2.rcode0.net - AUTHORITATIVE NAME SERVER**) in 31 ms

dig domen.hu +trace

```
.           511184  IN    NS    a.root-servers.net.
.           511184  IN    NS    b.root-servers.net.
.           511184  IN    NS    c.root-servers.net.
.           511184  IN    NS    d.root-servers.net.
.           511184  IN    NS    e.root-servers.net.
.           511184  IN    NS    f.root-servers.net.
.           511184  IN    NS    g.root-servers.net.
.           511184  IN    NS    h.root-servers.net.
.           511184  IN    NS    i.root-servers.net.
.           511184  IN    NS    j.root-servers.net.
.           511184  IN    NS    k.root-servers.net.
.           511184  IN    NS    l.root-servers.net.
.           511184  IN    NS    m.root-servers.net.
```

511184 IN RRSIG NS 8 0 518400 20201128050000 20201115040000 26116 . Ylch67Ac85HtLazykdEeE6a8Y2misXyjsatG75PbfvJOlqYP8NK0gEkN Lwm7eAv3wlgxg681w63YeCQgvywbvOULIz+Kq0/p0z/TWEXDKvdjDtuR xdPMi+JdUTDoBJEMJbn/8IMFmgCPg5+zxIg+TDDcJvbKiyaLCv2QZ2Y+ cAcKroPkhD1SJ7fCJNXzTTklPkcOVhrQCsc1QB+s30wWjtA33mlu/FLz Iosji2e5rVrsi31UEMW+C0wjLuHQOfzHJoN0qed2z/zUW04G0xOLcKP+ SwBrxMOczHh2H+7jZMoiWED+NICgqGbvG7WPQQisryCxW6y1OkKRq8jH BmirqA==

hu. 172800 IN NS e.hu.

hu. 172800 IN NS d.hu.

hu. 172800 IN NS ns2.nic.fr.

hu. 172800 IN NS b.hu.

hu. 172800 IN NS ns-com.nic.hu.

hu. 172800 IN NS c.hu.

hu. 172800 IN NS **a.hu.**

hu. 86400 IN DS 2104 8 2 65F5D64B860F26FEAE0BDE3CA51B730B38381678C8C316F16B37E551 105EBAC5
hu. 86400 IN DS 20056 8 2 93FDCE134B52B1BBFDCADDAD9152B0F2CA6E9DEE09150DF624661C6B 9A5B74DA
hu. 86400 IN RRSIG DS 8 1 86400 20201128050000 20201115040000 26116 .
HKgJXcG1NTvmw9wDbwQtinYB8mX/yxhBmvCILoHxmJ3/mpdGTh5mgIz5 wHT83KPzVNIyr6ILo97iMSM2q1i7q3lB1A/RhlnCqft8b6Hg0s7C28wA
1dY1Nre0yH61MXEL9s02fdmCCMZx1QbNnCYEksPALMMvcKA0Rd0Gs+4E crepDH7eT7RPMayK0vFtv4b/JBJ7lMdm1O/mEFZdFKlgw/XjulsLuZf5
GkATehygbNHhXHFHYACB3t+t7FiZJEjJTuDqupTW1PvAoNCsLRiqEGRG 50HVQP/ioyV9D6F1l5+a5OypurGsxcWM3/VbFs0lNpu9GI5GmNGyvM9A 4OpmLA==

```
domen.hu.       86400   IN      NS      sec2.rcode0.net.
domen.hu.       86400   IN      NS      secondary.dns2.hu.
domen.hu.       86400   IN      NS      pns102.cloudns.net.
domen.hu.       86400   IN      NS      pns103.cloudns.net.
domen.hu.       86400   IN      NS      udns1.hu.
domen.hu.       86400   IN      NS      pns101.cloudns.net.
domen.hu.       86400   IN      NS      ns103.cloudns.net.
domen.hu.       86400   IN      NS      sec1.rcode0.net.
domen.hu.       86400   IN      NS      ns104.cloudns.net.
domen.hu.       86400   IN      NS      pns104.cloudns.net.
domen.hu.       86400   IN      NS      ns102.cloudns.net.
domen.hu.       86400   IN      DS      9386 8 2 1511E4B325F61208B90687593B4DA275C3C9C3E317DD17085408E520 E72EAAD2
domen.hu.       86400   IN      DS      64891 8 2 8D38C7F6B4F557A91CD9751BF216D5DBC98DFEF595D9FEF1D0DB9A7C C925D1A7
domen.hu.       86400   IN      RRSIG   DS 8 2 86400 20201203004205 20201104183055 55779 hu.
iLbtTDjcDkah5aI62K4yoes5b1HVewNTPFzAH7BjiFqYb4ZLwFwV4ciV NPxJhAvukAAJr5LRh5BRtznEHqQFwHb33VUZwxvQKP/UdHrQeo10K+63
X6I1ZkuCllH+0bQlGuIvu6IuwSxplIKlFgOOTUPwsKsq1aqIQ+lWb/sS zb4=
```

domen.hu. 60 IN A 212.52.164.124

```
domen.hu.       60    IN    RRSIG   A 8 2 60 20201123012632202011130026 32 13080 domen.hu.
D3Cvu5VrSa3FvLYXHRlAjNvzJ9vcHGBvQ2xss9SScCwf3bJnIonQcxHq eQEDnWAnLV0eMO4Uw1jyvDCeLm0laGfQc6ybUTK4oQr0Q11DKBJNFYgg
+gagqzdOdM9hU2knLCGoDshrY9/nRJav3rO0h5F1D5IuHBYz0mAnJCcS ZE4=
domen.hu.       300   IN    NS    ns103.cloudns.net.
domen.hu.       300   IN    NS    sec1.rcode0.net.
domen.hu.       300   IN    NS    pns103.cloudns.net.
domen.hu.       300   IN    NS    pns104.cloudns.net.
domen.hu.       300   IN    NS    ns104.cloudns.net.
domen.hu.       300   IN    NS    pns102.cloudns.net.
domen.hu.       300   IN    NS    ns102.cloudns.net.
domen.hu.       300   IN    NS    sec2.rcode0.net.
domen.hu.       300   IN    NS    secondary.dns2.hu.
domen.hu.       300   IN    NS    pns101.cloudns.net.
domen.hu.       300   IN    NS    udns1.hu.
domen.hu.       300   IN    RRSIG   NS 8 2 300 20201123163632 20201113153632 13080 domen.hu.
MnVGvdoqbeqyR5t/ggUJ4xFFYSYp8vqwvsrZGQS11NXgE47HcVqh+Or7 PJABhE/fKJUA+JCnvaJCBbCBVYIShnZxgnWPMu4wIgcP58CZzPKYCCx3
PK7tpzs0V0PJ1JC693N6M48kHne9v/RSU/QNRots8Df1EuE7JUHRy+3y ja8=
;; Received 638 bytes from 108.59.1.30#53(ns102.cloudns.net)
```

```
www.domen.hu.        60    IN    A     212.52.164.124
www.domen.hu.        60    IN    RRSIG   A 8 3 60 20201123012632 20201113002632 13080 domen.hu.
Uf1/WPPyxGJF6FFfoxb4OzlI3LweXW6POdXjsv2bUtPTaaUDMMgXFZOx
qxMY3TjhLPjXlGh98rJAu0OT9vHQi1IATozyFeOaKiQLc/Co979GoDr4
ZR0Y3RlJ/Kvstc+unYQgm1ccgQzV1H9jEzyWXOucIQybj3eWPP3hdotB 6q8=
domen.hu.            300   IN    NS    pns101.cloudns.net.
domen.hu.            300   IN    NS    pns102.cloudns.net.
domen.hu.            300   IN    NS    ns104.cloudns.net.
domen.hu.            300   IN    NS    ns103.cloudns.net.
domen.hu.            300   IN    NS    secondary.dns2.hu.
domen.hu.            300   IN    NS    ns102.cloudns.net.
domen.hu.            300   IN    NS    udns1.hu.
domen.hu.            300   IN    NS    pns103.cloudns.net.
domen.hu.            300   IN    NS    sec2.rcode0.net.
domen.hu.            300   IN    NS    pns104.cloudns.net.
domen.hu.            300   IN    NS    sec1.rcode0.net.
domen.hu.            300   IN    RRSIG   NS 8 2 300 20201123163632 20201113153632 13080 domen.hu.
MnVGvdoqbeqyR5t/ggUJ4xFFYSYp8vqwvsrZGQS11NXgE47HcVqh+Or7
PJABhE/fKJUA+JCnvaJCBbCBVYIShnZxgnWPMu4wIgcP58CZzPKYCCx3
PK7tpzs0V0PJ1JC693N6M48kHne9v/RSU/QNRots8Df1EuE7JUHRy+3y ja8=
;; Received 642 bytes from 108.59.1.30#53(ns102.cloudns.net)
```

DNSSEC

Az ilyen szituációk megakadályozására szolgál a DNSSEC:

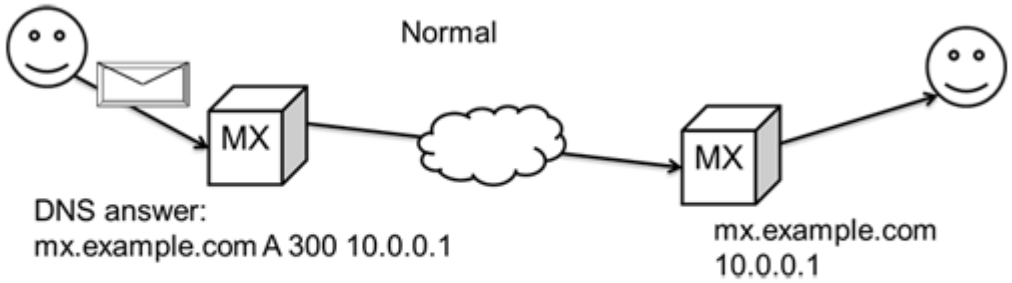


Figure 1: A usual mail handling path following a usual DNS answer

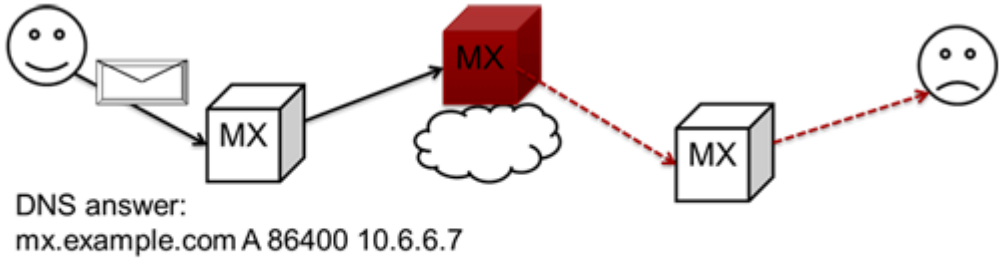


Figure 2: A mail handling path hijacked via DNS cache poisoning

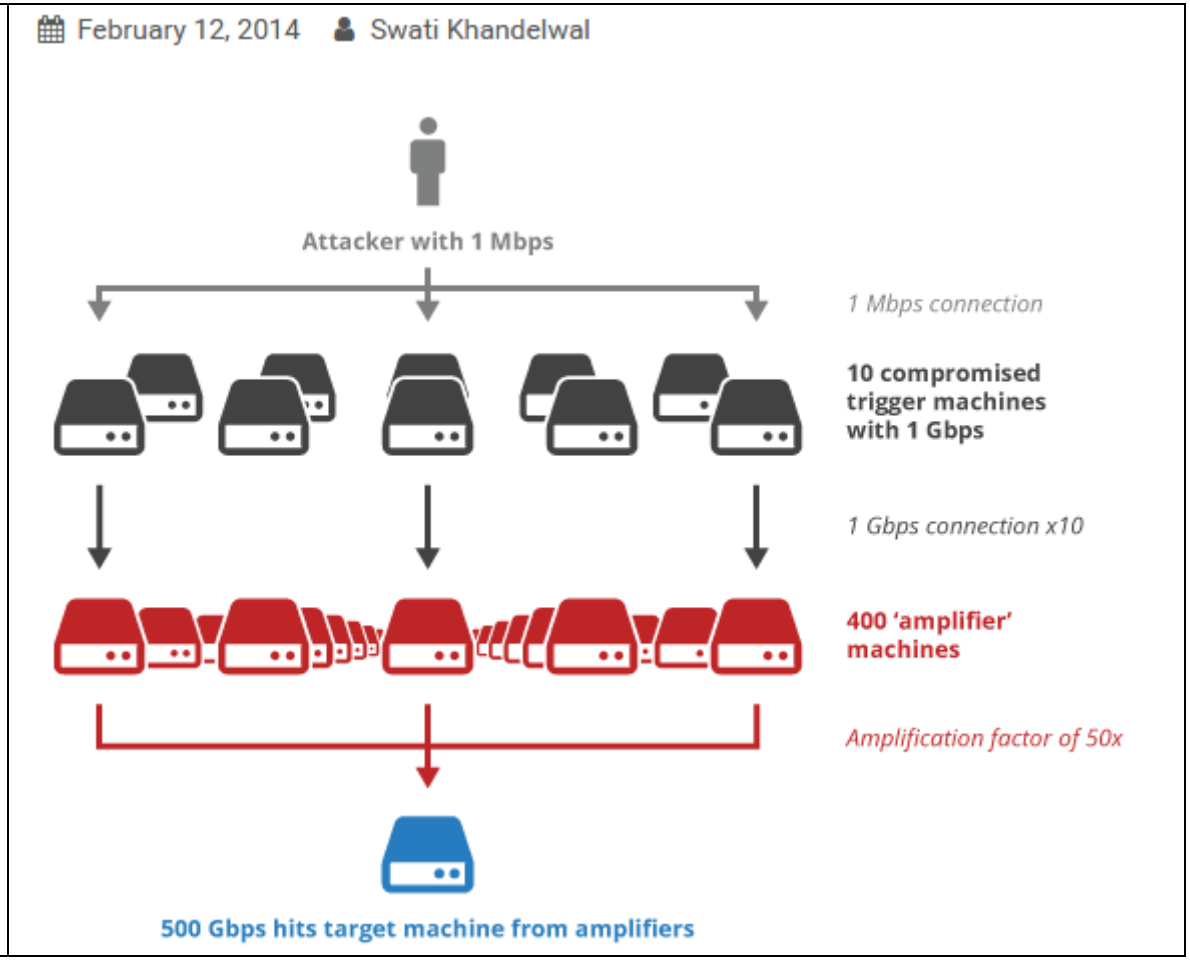
https://insights.sei.cmu.edu/cert/2014/09/-probable-cache-poisoning-of-mail-handling-domains.html?utm_referrer=https://www.google.com/

https://www.iana.org/dnssec/ceremonies
https://www.internetsociety.org/blog/2015/11/my-view-of-the-dnssec-root-key-signing-ceremony/

DoS/DDoS

- DoS
- DDoS
- botnet
- erősítéses támadások

- DDoS-mitigáció



https://thehackernews.com/2014/02/NTP-Distributed-Denial-of-Service-DDoS-attack.html

Amazon reported sustaining a 2.3 Tbps DDoS attack in 2020

Ma tárgyalt további fogalmak

Unicast és anycast routing, ill. unicast és anycast DNS

Domain hijacking (doménlopás)

Registry Lock

Tanúsítványrekordok (pl. CAA, CERT stb.)

E-mail authentikáció: SPF, DKIM, DMARC

Elektronikus aláírás fogalmai

Biztonsági incidens

Folytassuk a tanulást!

9.30-tól:

- Hogyan válasszunk domainnevet?
- Domain portfolió menedzsment
- Honnan érhet támadás, ártalom? Hogyan lopjunk el domain nevet?

…