DNSSEC

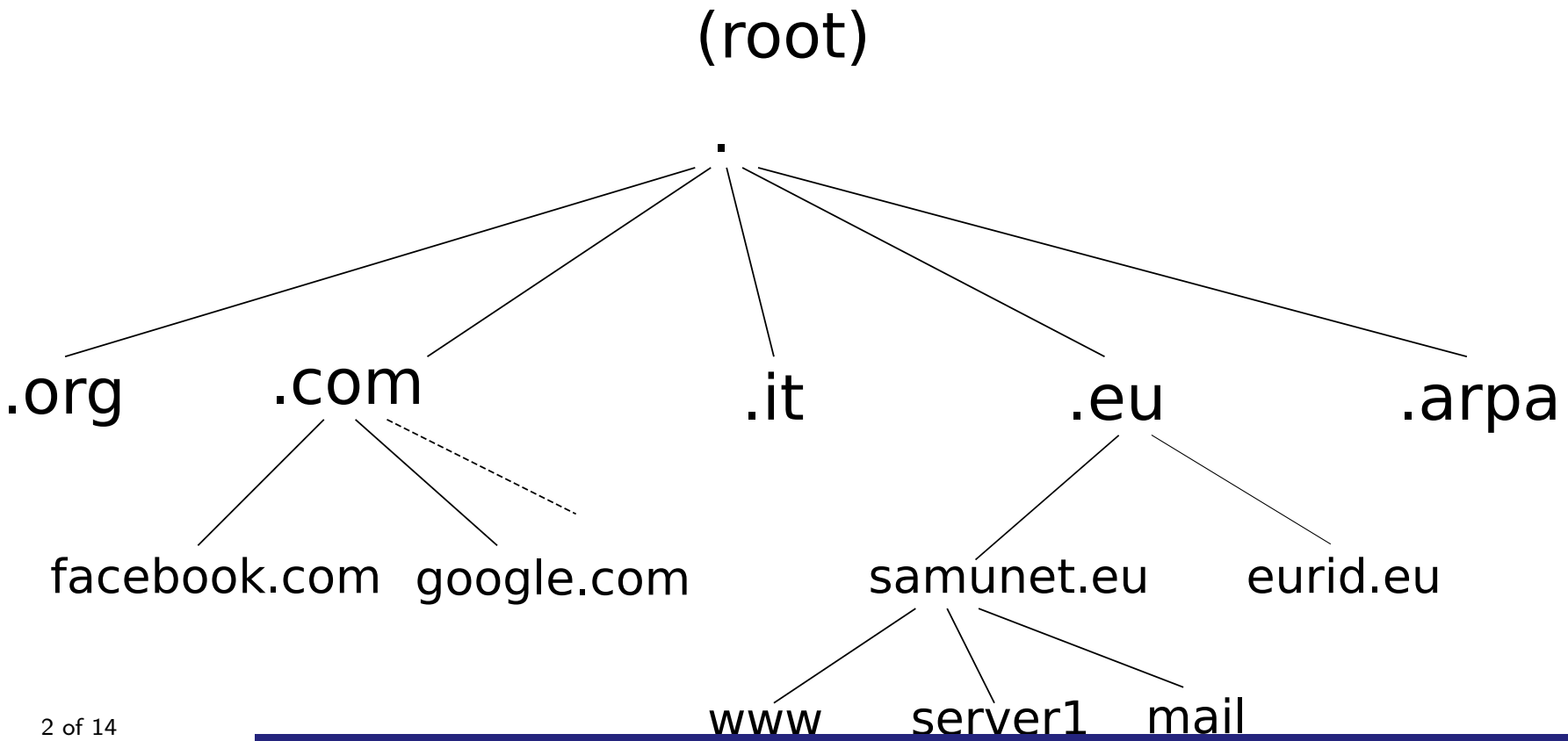
a real, working and optimized implementation

Samuele Racca
samuele.racca@polito.it

Politecnico di Torino
TOP-IX

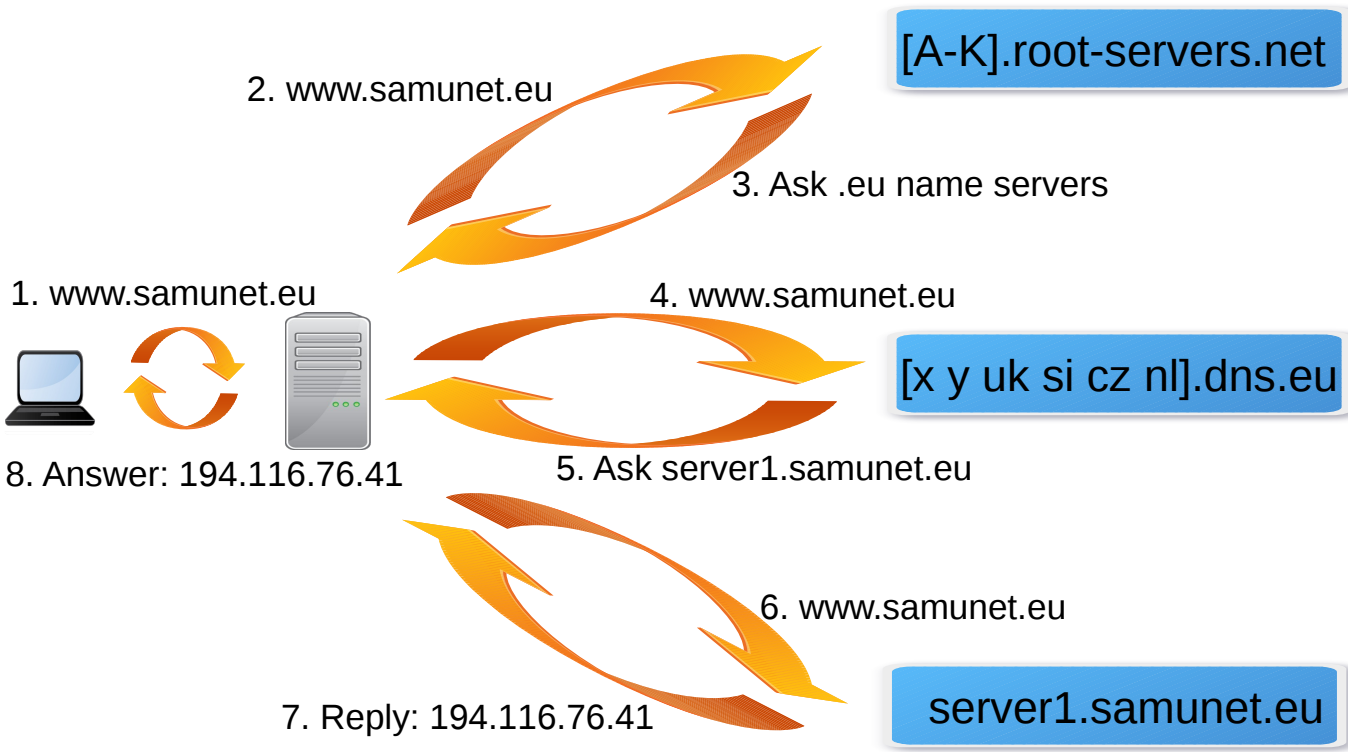
Basic DNS

Il DNS (Domain Name System) è uno dei protocolli fondamentali alla base di Internet, sviluppato per associare i nomi delle risorse di Internet agli indirizzi IP dei server che le ospitano (*record*).
Oggi senza DNS Internet non potrebbe funzionare.



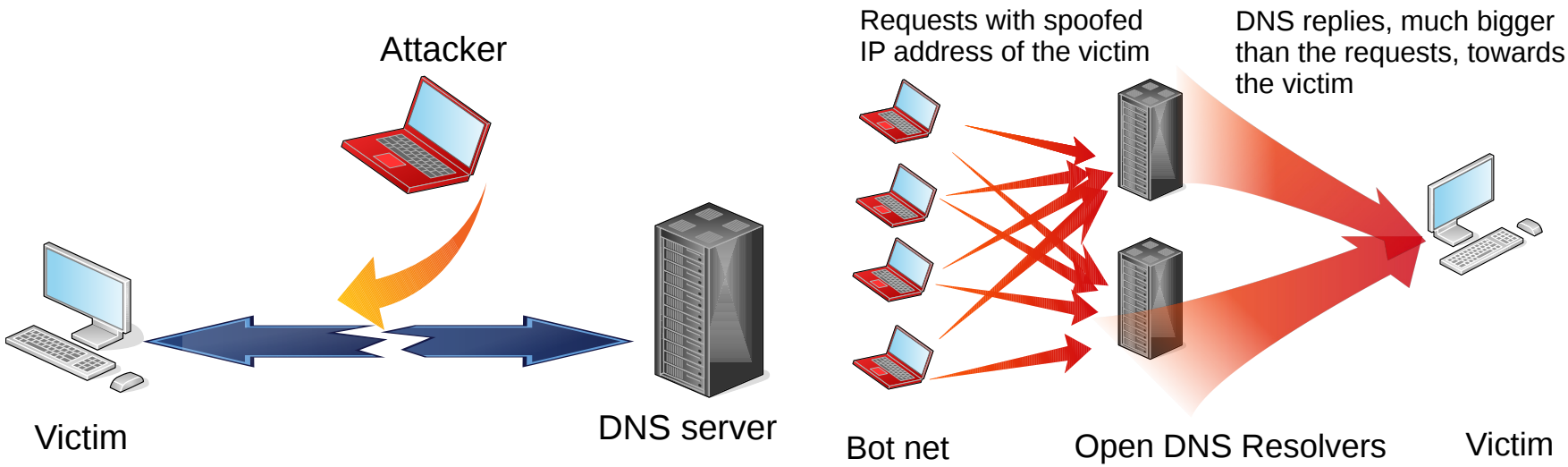
Basic DNS

Il DNS (Domain Name System) è uno dei protocolli fondamentali alla base di Internet, sviluppato per associare i nomi delle risorse di Internet agli indirizzi IP dei server che le ospitano (*record*).
Oggi senza DNS Internet non potrebbe funzionare.

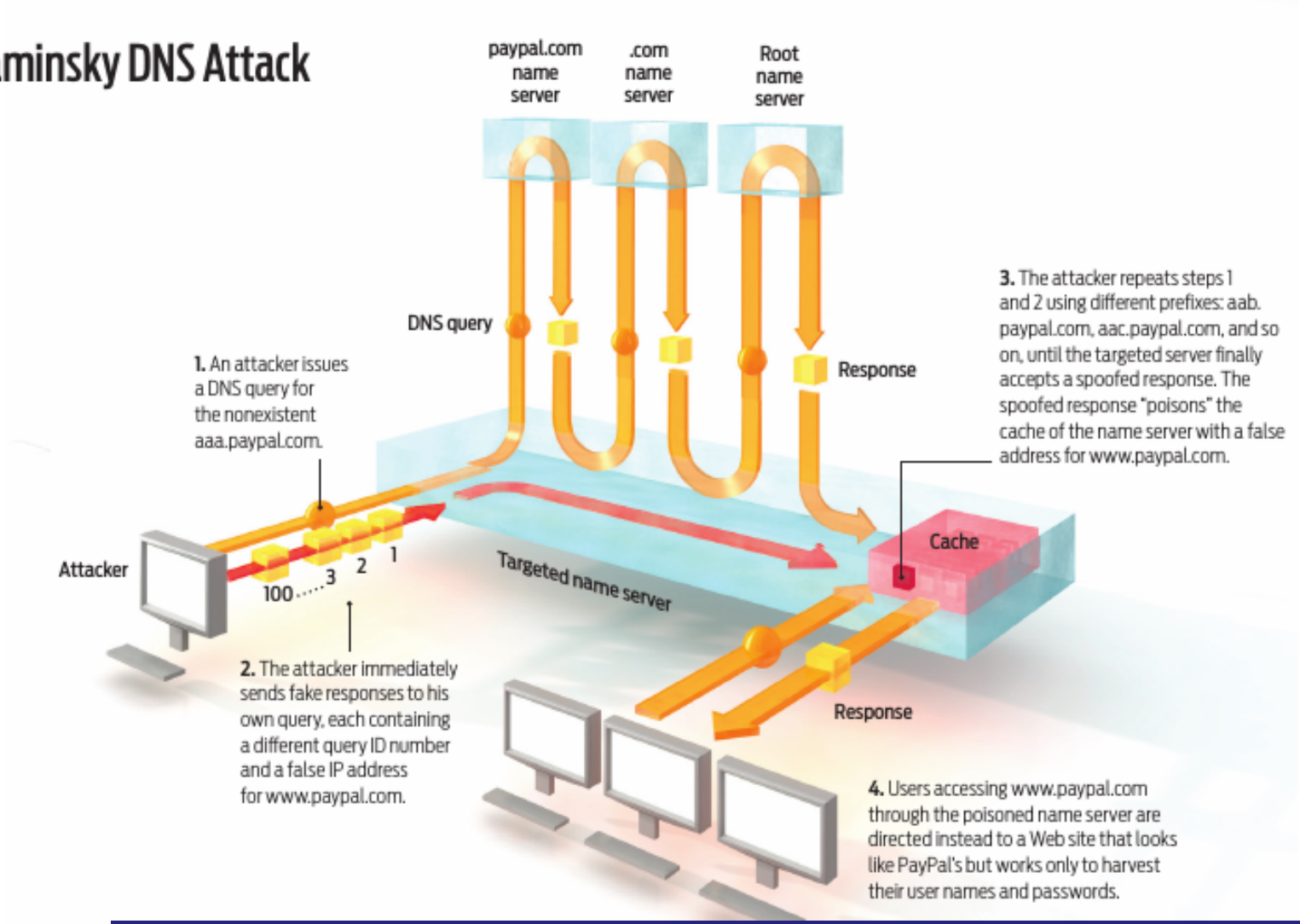


Problemi di sicurezza del DNS

- **DNS hijacking**
  Un attaccante modifica i pacchetti nella comunicazione tra un utente e il server DNS, senza che l'utente se ne accorga
- **DNS amplification attack**
  Vengono sfruttati degli *open resolvers* per amplificare un attacco DDoS



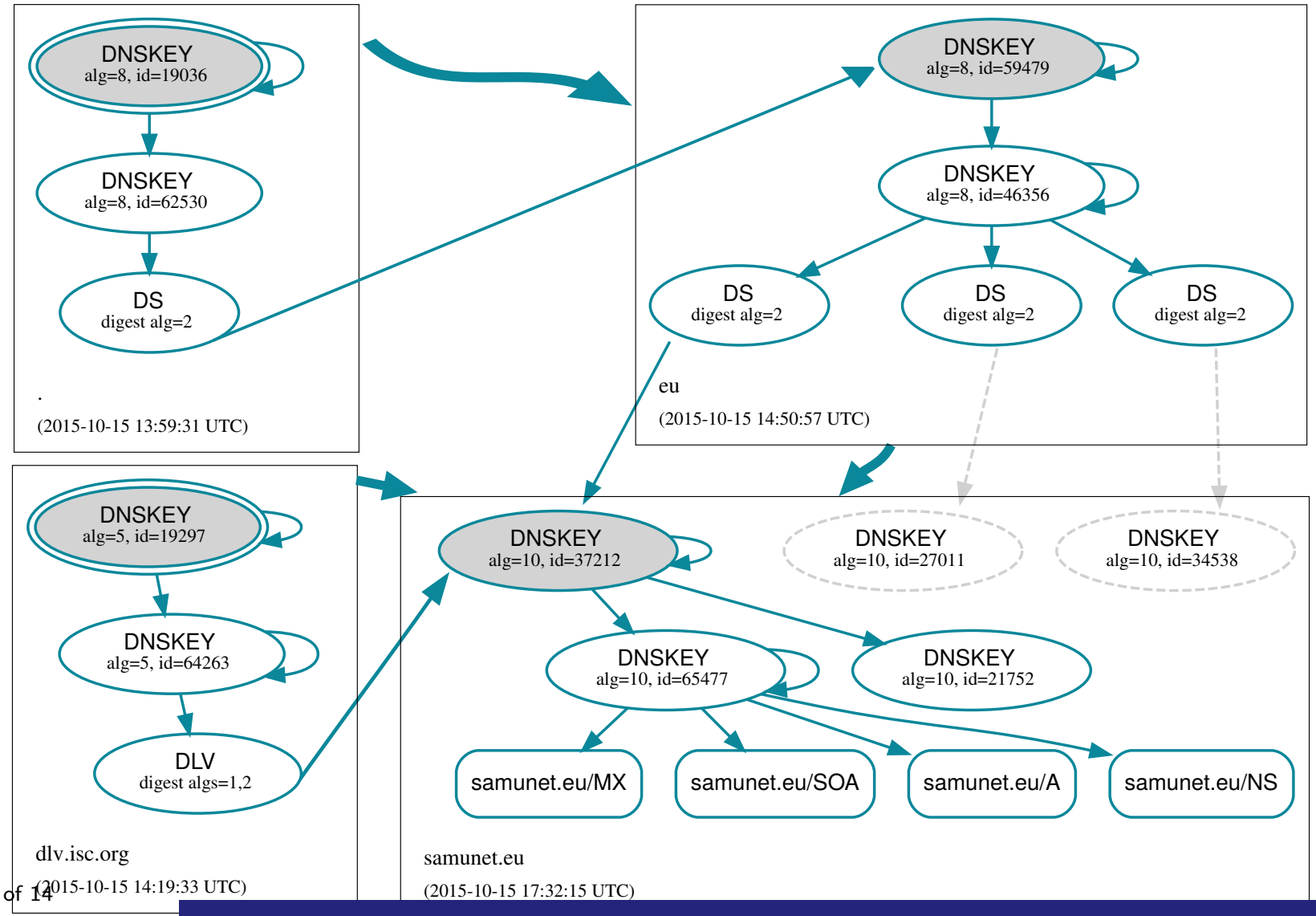
- **DNS cache poisoning e la vulnerabilità di Kaminsky**
  Un attaccante inserisce nella cache del server DNS associazioni malevole per redirigere gli utenti altrove o per rubare l'intero dominio.



DNSSEC

- estensione del protocollo DNS base, retro compatibile
- autenticazione ed integrità tramite un sistema crittografico a chiave pubblica, simile alla firma digitale
- non esistono CA perché le chiavi sono gestite in maniera indipendente
- due tipi di chiavi: KSK (Key Signing Key) e ZSK (Zone Signing Key)
- è possibile utilizzare diversi algoritmi standard: RSA, DSA, DH, ECDSA, MD5, SHA-1, SHA256 and SHA512
- autenticazione per la non esistenza dei nomi
- nuovi tipi di record:
  - DS, DLV
  - DNSKEY
  - RRSIG
  - NSEC e NSEC3

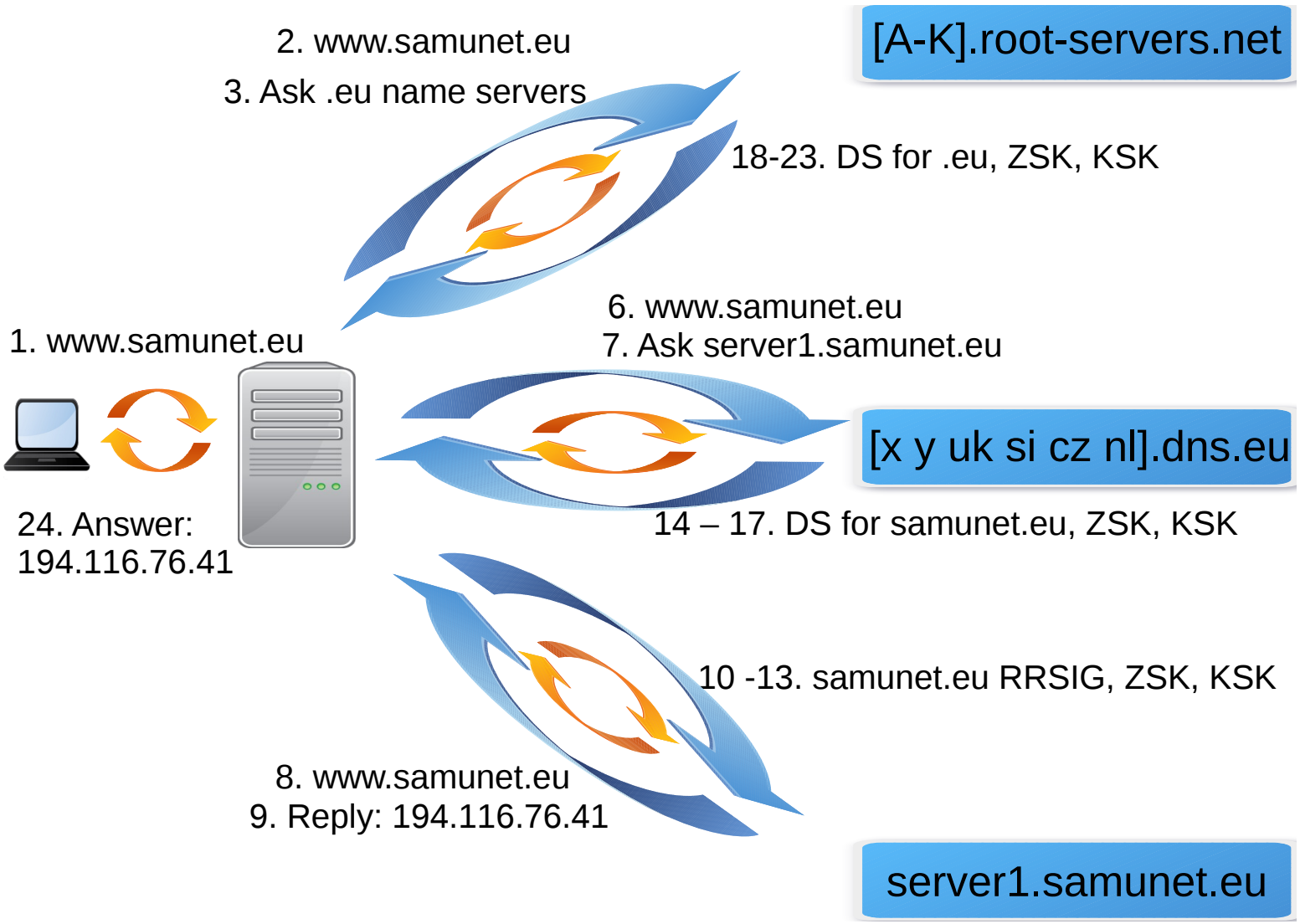
samunet.eu the working example



KSK and ZSK

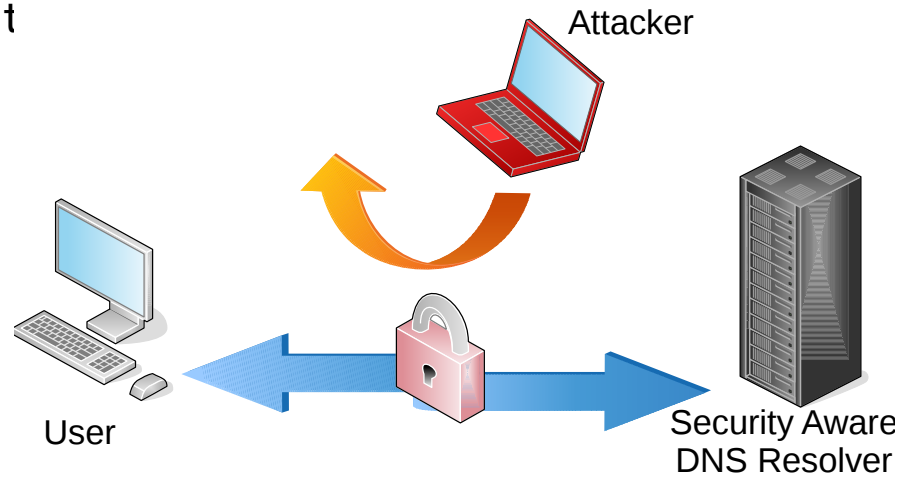
- la ZSK firma i records
- la KSK firma le ZSKs
- la *Catena della Fiducia*
- le procedure di *Rollover* per il cambio di chiavi
  - doppia firma delle zone
  - pre-pubblicazione della chiave
- i tempi del DNSSEC
  - TTL dei record
  - durata delle firme
  - durata delle chiavi

La Risoluzione con il DNSSEC



Sicurezza nella comunicazione utente-server DNS

- il DNSSEC dà regole generali per rendere sicura la connessione fra utenti e server DNS di riferimento
- non c'è uno standard
- `samunet.eu` sfrutta DNSCrypt-proxy
  - versione server e client
  - cross platform, disponibile anche per dispositivi mobili
  - sviluppato da OpenDNS, ora acquisita da Cisco
  - crittografia a chiave pubblica
  - attualmente mantenuto e sviluppat



Il meccanismo DLV

- DNSSEC Look-aside Validation
- l'unico database di record DLV è gestito dall'ISC: `dlv.isc.org`
- utilizzato per creare la *Catena di Fiducia* per quei domini il cui dominio di livello superiore non supporta DNSSEC
- nato lal'inizio della sperimentazione del DNSSEC
- attivo fino a metà 2017
  - 79% dei TLD sono firmati
  - la zona radice è firmata
  - riduce le richieste ai TLDs
  - genera molto traffico aggiuntivo e inutile[1]

[1] https://ripe70.ripe.net/presentations/81-RIPE-DLV-timeline-20150513.pdf

Analisi di sicurezza

Pro

- protezione da attacchi Man-In-The-Middle e che sfruttano la vulnerabilità di Kaminsky
- sicurezza contro cache poisoning
- protezione attiva dell'utente tramite negazione delle risorse
- certezza delle risorse alle quali si accede

Contro

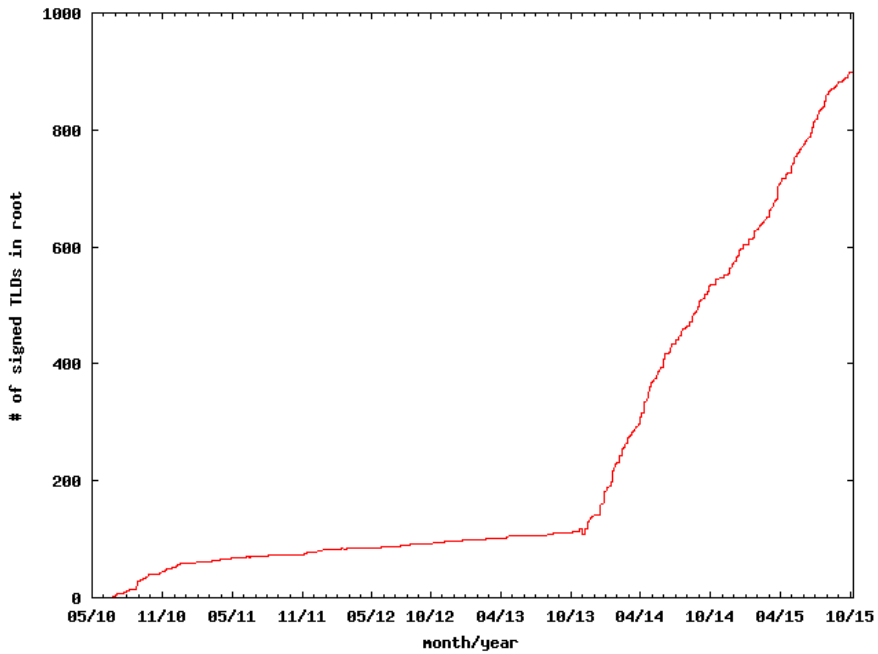
- il DNS amplification attack diventa più pericoloso
- la gestione dei tempi diventa cruciale
- attacco di Zone-Walking (risolto implementando NSEC3)

Prestazioni

Non può esserci sicurezza senza una maggiore complessità e lo spreco di risorse.
Il DNSSEC richiede più risorse rispetto al DNS:

- spazio di archiviazione
  - chiavi
  - firme
- banda
  - DNS: 10 pacchetti - 4267 Bytes
  - DNSSEC: 24 pacchetti - 10363 Bytes
  - DNSSEC e canale sicuro utente-server DNS: 121 pacchetti - 52253 Bytes
- capacità di elaborazione

La situazione attuale



- la zona radice è firmata
- dal 2008 i domini *.gov* sono firmati
- *.eu* è firmato, ma *.it* non ancora
- sono già state configurate 4568 zone[a]
- utilizzo in crescita
- `samunet.eu` è firmato, operativo, verifica i record DNS e permette connessioni sicure verso i propri server autoritativi

[a] According to ISC

Conclusioni

- con un overhead abbiamo:
  - certezza delle risorse alle quali si accede
  - protezione attiva per gli utenti
  - protezione per i gestori di domini
  - protezione dal *phishing*
- fondamentale per *secureBGP* e fortemente consigliato per IPv6
- un passo obbligato verso una rete più sicura e neutrale