# Il programma MORECOWBELL della NSA

## Campane a morto per il DNS

Christian Grothoff (INRIA Rennes),
Matthias Wachs (Technische Universität München),
Monika Ermert (Heise),
Jacob Appelbaum,
*Traduzione italiana di Luca Saiu*

Gennaio 2015



## 1 Introduzione

Quasi ogni interazione sulla rete inizia con una richiesta al Domain Name System (DNS, sistema dei nomi di dominio), un protocollo Internet centrale che permette agli utenti di accedere ai servizi Internet per nome, per esempio scrivendo `www.example.com` invece di usare un indirizzo IP numerico come 2001:DB8:4145::4242. Sviluppato "ai vecchi tempi di Internet" il DNS contemporaneo ricorda un grosso diagramma delle attività in rete per ciechi. Di conseguenza il DNS non solo attrae ogni sorta di sorveglianza motivata commercialmente ma, come confermano i documenti del programma di spionaggio MORECOWBELL[1] della NSA (la National Security Agency americana), anche la NSA stessa. Date le debolezze di progetto del DNS, questo pone una questione: il DNS può essere reso sicuro e salvato, oppure deve essere interamente sostituito almeno in alcuni casi d'uso?

Gli ultimi due anni hanno visto un picco di attività nel tentativo di ottenere sicurezza e privacy nel DNS da parte della Internet Engineering Task Force (IETF), il corpo che documenta gli standards DNS. La Internet Architecture Board, un organismo parallelo alla IETF, ha semplicemente suggerito agli ingegneri di adottare la crittografia a ogni livello, includendo potenzialmente anche il DNS [2].

Una bozza recente [4] della IETF sulla privacy del DNS comincia riconoscendo che il DNS

> "... è uno dei componenti infrastrutturali più importanti di Internet e uno tra i più ignorati o fraintesi. Quasi ogni attività su Internet inizia con una richiesta al DNS (e spesso più di una). Il suo uso ha molte implicazioni sulla privacy ..."

Malgrado questa presa d'atto sia apparentemente condivisa da tutti, la IETF non si aspetta che le soluzioni attuali dell'industria cambieranno la situazione a breve termine:

> "La possibilità di una cifratura massiccia del traffico DNS appare ad oggi molto remota." [3]

[1] *Nota del traduttore:* il modo di dire "more cowbell" richiama uno sketch comico del *Saturday Night Live* in cui un produttore discografico continuava parossisticamente a chiedere "più campanaccio" al gruppo che stava registrando. Nel linguaggio popolare americano qualsiasi problema si risolve aggiungendo "more cowbell".

Dal punto di vista della sorveglianza il DNS attualmente tratta tutta l'informazione del database DNS come se fosse pubblica. Il contenuto delle richieste e delle risposte è tipicamente in chiaro. Questo permette agli *attaccanti passivi* di monitorare le richieste degli utenti e osservare quali siti web stiano visitando. Per un *attaccante attivo* il DNS aiuta a localizzare dei servizi potenzialmente vulnerabili, il che costituisce il primo passo per la loro intrusione attraverso gli attacchi 0-day disponibili in commercio.

Le discussioni recenti all'interno della IETF includono proposte per la "minimizzazione delle richieste", DNS confidenziale, DNS sopra TLS, DNSCurve, e altre proposte più radicali di sistemi di nomi alternativi che migliorino la privacy. Ognuna di queste proposte adotta un approccio diverso per ridurre il ruolo del DNS come la fonte finale di meta-dati, nel panopticon digitale conosciuto come Internet.

## 2 MORECOWBELL: spiare il traffico DNS

Dato lo stato attuale del DNS simile a un libro aperto non è sorprendente che un nuovo gruppo di documenti top secret verificati da Heise abbia rivelato come il programma MORECOWBELL (MCB) dell'agenzia americana di spionaggio NSA esegua un monitoraggio sul DNS come una fonte di informazioni su Internet (Figura 2). Il programma MORECOWBELL della NSA impiega un'infrastruttura dedicata segreta per interrogare attivamente i servers DNS ed eseguire richieste HTTP al fine di ottenere meta-dati sui servizi e controllare la loro disponibilità.

Malgrado la natura aperta del DNS la NSA esegue tutto questo di nascosto (Figura 3) per assicurarsi che migliaia di richieste DNS ogni ora non siano attribuite al governo degli Stati Uniti; i servers affittati dalla NSA allo scopo di monitorare il DNS e controllare i servers web via HTTP sono infatti situati fisicamente in Malaysia, Germania e Danimarca (Figura 4) il che permette alla NSA di osservare in modo coperto, e di ottenere una visione più globale della risoluzione dei nomi da parte del DNS e della disponibilità dei servizi. Mentre i lucidi elencano solo questi tre paesi, l'infrastruttura sconosciuta PACKAGEDGOODS sulla quale MORECOWBELL è costruito è nota per comprendere macchine in almeno 13 altri paesi, come descritto precedentemente da Der Spiegel in un insieme di lucidi che descrivono il programma NSA TREASUREMAP [13].

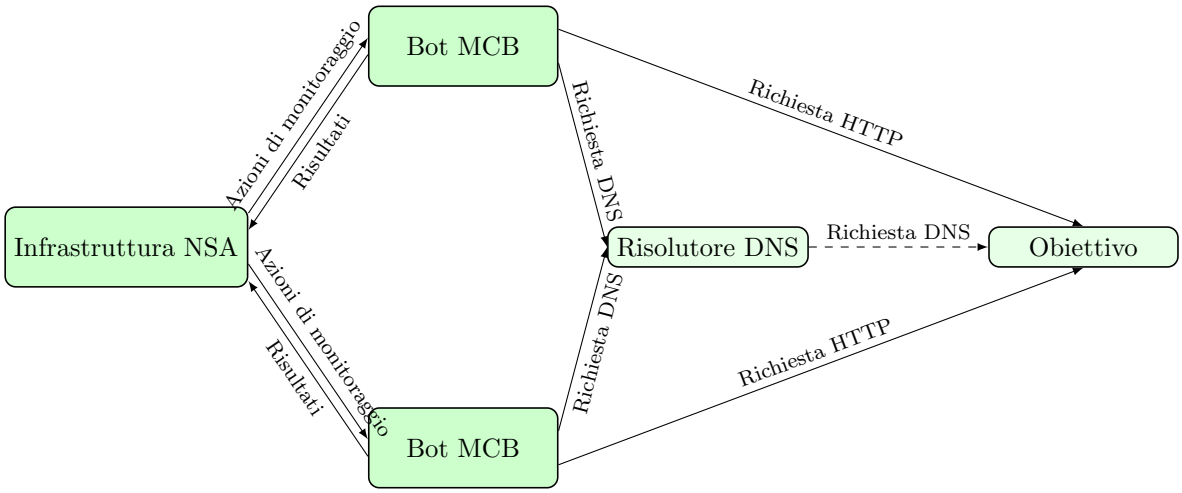



Figura 1: L'infrastruttura MORECOWBELL della NSA: una lista di obiettivi da monitorare viene inviata a dei bots distribuiti geograficamente, che eseguono dichieste DNS e HTTP su dei siti web per ottenere informazioni sulla disponibilità dei servizi. I dati ottenuti sono reinviati alla NSA a intervalli regolari.

Il punto interessante è la mancanza di interesse da parte della NSA a proposito del contenuto specifico dei servers web e delle entries di DNS — la NSA è alla ricerca di *meta*-dati: vuole sapere se l'informazione sul DNS è cambiata, e verificare la disponibilità del servizio. I lucidi mostrano come questi semplici controlli abbiano anche utilizzi piuttosto benigni, come ad esempio monitorare alcuni dei siti web dello stesso governo americano. Osservando i cambiamenti a livello di DNS un attacco diventa possibile ripetere un attacco nel caso in cui una vittima decidesse

di spostare i suoi servizi verso un altro sistema o un'altra rete. Mantenendo l'infrastruttura di monitoraggio coperta e distribuita geograficamente l'NSA ottiene una visione globale dell'impatto di un attacco. Questo rende più difficile per le vittime identificare i servers che osservano, la qual cosa potrebbe altrimenti permettere loro di evitare un attacco trattando in modo diverso le richieste da parte dei servers che li osservano, un approccio usato comunemente con DNS e chiamato *split view* (visione separata).

Per quanto non abbiamo prove di tale comportamento, il termine "battle damage indication" (indicazione di danni di battaglia) potrebbe anche includere "danni" provenienti da origini diverse dagli attacchi digitali, ad esempio raids di bombardamento o cavi tagliati. Il governo statunitense utilizza il termine "battle damage indication" per attacchi cinetici:

> "INDICAZIONE DEI DANNI DI BATTAGLIA
>
> Lo scopo di questo lavoro è sviluppare metodi innovativi a basso costo per determinare velocemente l'effetto che una munizione via aria ha avuto sul suo obiettivo atteso. Ciò è particolarmente importante nel caso di obiettivi sepolti in profondità dove le indicazioni visuali possano risultare difficili da percepire. Un collegamento dati di bordo con le munizioni può essere appropriato per ottenere un'indicazione dei danni a questo tipo di obiettivi.
>
> Un simile collegamento dati può consistere in un cavo, o può essere completamente wireless. D'altra parte, l'**indicatore dei danni di battaglia** può essere del tutto indipendente dalla munizione che penetra. Lo scopo di questo studio è svoluppare un mezzo a basso costo, efficiente e affidabile per fornire rapidamente al combattente una determinazione accurata, o almeno una stima affidabile, del danno inflitto a un obiettivo – particolarmente uno rinforzato o sepolto in profondità.
>
> —Dr. Alex Cash AFRL/MNMI (850) 882-0391 `cash@eglin.af.mil`"[2]

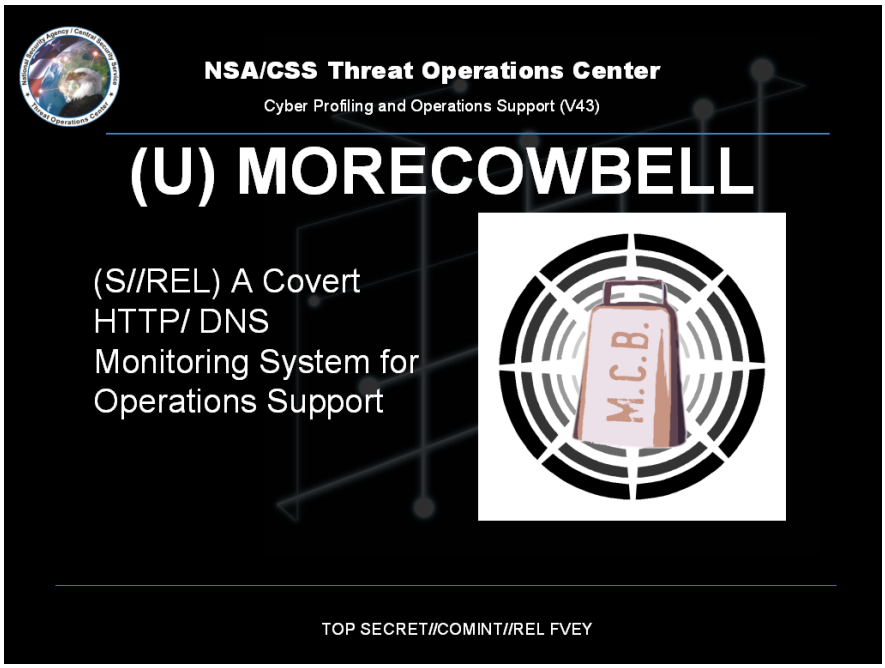



Figura 2: MORECOWBELL: un sistema coperto per il monitoraggio HTTP/DNS

I vari documenti della NSA a proposito del DNS mostrano che gli attacchi coperti esistenti sul DNS vanno oltre la sorveglianza di massa, e hanno un ruolo di supporto per gli attacchi attivi [18]. Attraverso le rivelazioni sulla

[2]Il grassetto è nostro. Citato secondo `http://www.darkgovernment.com/airforcedev.html`.

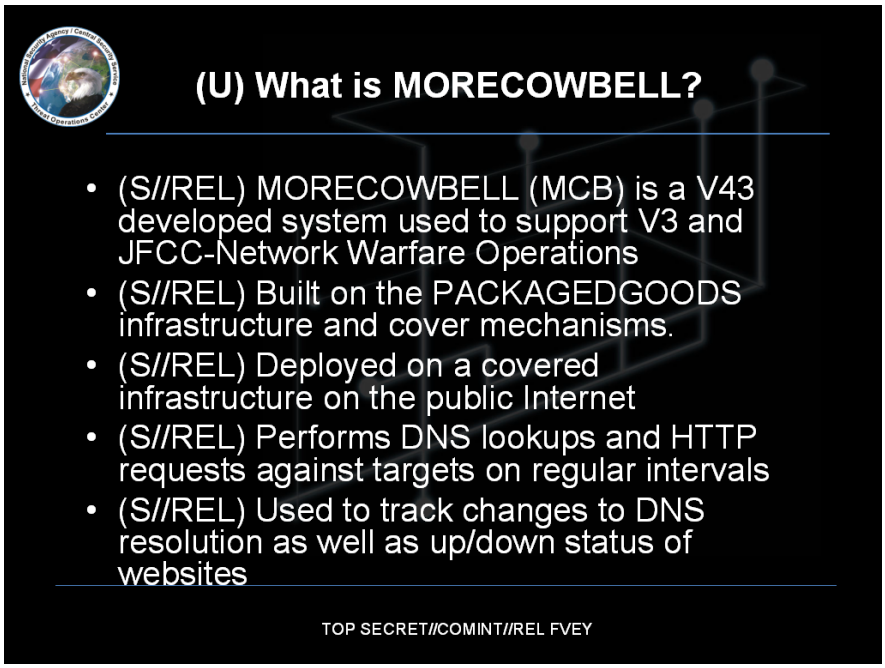



Figura 3: Cos'è MORECOWBELL.

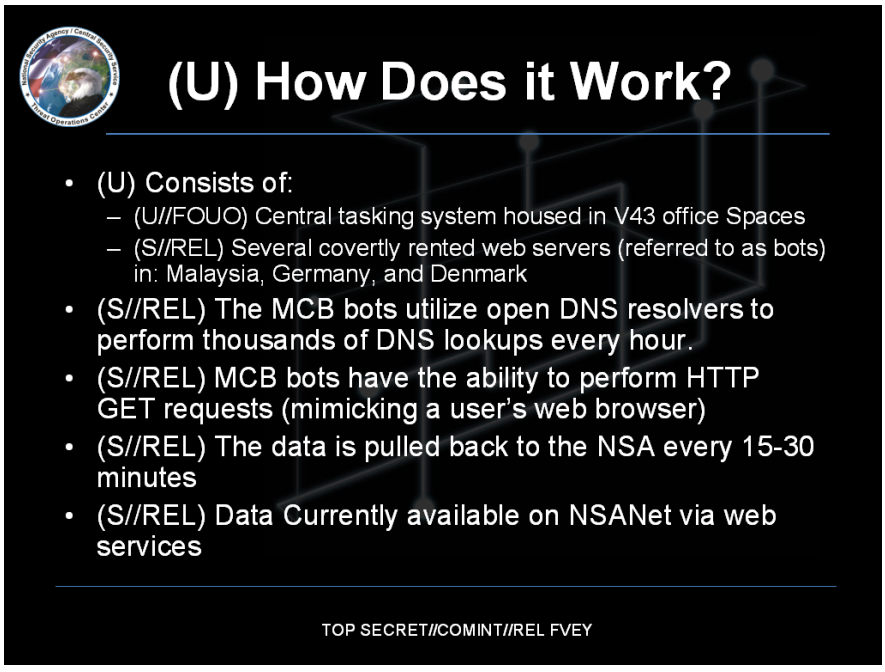



Figura 4: Come funziona MORECOWBELL?

sulla famiglia di progetti di NSA QUANTUMTHEORY con sotto-progetti come QUANTUMDNS, sappiamo che degli attaccanti potenti come stati nazionali sono in grado non solo spiare il traffico DNS, ma anche di iniettare

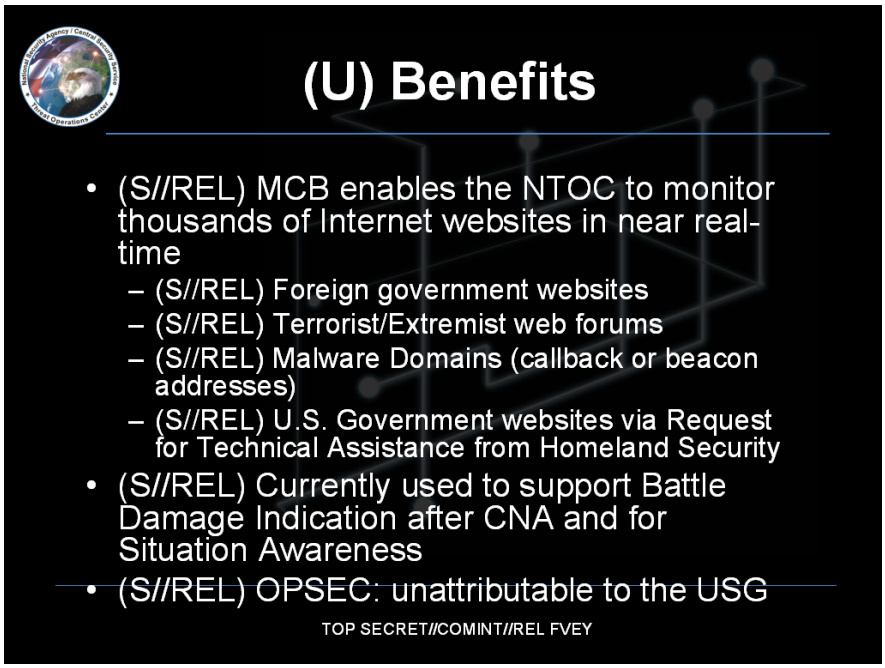



Figura 5: "Benefici" di MORECOWBELL.

disposte DNS per modificare il risultato della risoluzione dei nomi, o farla completamente fallire [14]. Poiché DNS non fornisce confidenzialità per proteggere la privacy, è molto facile creare un profilo degli utenti e del loro comportamento durante la navigazione sul web. Questa informazione può poi essere usata anche per eseguire attacchi QUANTUMTHEORY contro l'obiettivo. I programmi NSA come QUANTUMBOT hanno lo scopo di monitorare le botnets IRC e individuare i computers che operano come bots per una botnet, dirottando i canali di comando e di controllo che servono per controllarli. Questi programmi sono giudicati *highly successful* nei documenti della NSA [12].

Di conseguenza la comunità Internet deve lavorare per risolvere i problemi di privacy e sicurezza nella risoluzione dei nomi in generale, e col sistema Domain Name System (DNS) attuale. Nel resto di questo articolo passeremo in rivista l'architettura DNS esistente e uno spettro delle proposte attuali che sono state avanzate per migliorare la sicurezza di questo servizio Internet critico.

## 3 Background: DNS

Il Domain Name System (sistema dei nomi di dominio, DNS) è una parte essenziale di Internet visto che fornisce un mapping da nomi delle macchine a indirizzi IP, permettendo agli utenti di lavorare con nomi che si possano ricordare. Il DNS è gerarchico e memorizza dei mapping nome-valore entro i cosiddetti *records*, in un database distribuito. I nomi consistono in *etichette* delimitate da punti. La radice di tutta la gerarchia è l'etichetta vuota, e l'etichetta più a destra in un nome è nota come il top-level domain (TLD, dominio di livello massimo). I nomi con un suffisso comune si dicono essere nello stesso *dominio*. Il *tipo di record* specifica quale tipo di valore sia associato con un nome, e un nome può avere molti records, con diversi tipi. Il tipo di record più conosciuto è il record "A", che mappa i nomi in indirizzi IPv4.

Il database DNS è partizionato in *zone*. Una *zona* è una porzione del namespace in cui la responsabilità amministrativa appartiene a una particolare autorità. Una zona ha autonomia illimitata nel gestire i record in uno o più domini. Comunque, e questo è molto importante, un'autorità può delegare la responsabilità per particolari *sotto-domini* ad altre autorità. Ciò è possibile grazie a un record "NS", il cui valore è il nome di un server DNS

dell'autorita per il sotto-dominio. La *zona radice* è la zona che corrisponde all'etichetta vuota. È gestita dalla Internet Assigned Numbers Authority (IANA, autorità per i numeri assegnati in Internet), attualmente messa in opera dalla Internet Corporation for Assigned Names and Numbers (ICANN, corporazione per i nomi e i numeri assegnati in Internet) sotto un contratto della National Telecommunications and Information Administration (NTIA, amministrazione nazionale delle telecomunicazioni e dell'informazione). A sua volta la NTIA è un'agenzia del dipartimento del commercio statunitense, e come tale essa ha un ruolo operazionale piccolo ma significativo: controlla ogni aggiunta e cambiamento al file della zona radice. Il contratto NTIA-IANA scadrà il 30 settembre 2015, e la NTIA ha annunciato la sua intenzione di allontanarsi progressivamente dal suo ruolo attuale, al fine di passare il controllo a un'organizzazione globale gestita pluralmente da "portatori d'interesse" multipli. La zona radice contiene dei records "NS" che specificano nomi per i servers DNS ufficiali per tutti i TLD, per esempio "`.it`" o "`.roma`".

I nomi nel DNS sono risolti per mezzo di *risolutori*. Molti sistemi operativi moderni non forniscono un'implementazione completa di un risolutore DNS, ma solo dei cosidetti *stub resolvers* (risolutori-monconi). Questi stub resolvers non risolvono i nomi direttamente ma inoltrano invece le richieste a un *forward resolver*, tipicamente fornito dall'ISP che fornisce servizio Internet, come mostrato nella Figura 6. Questi risolutori risolvono il nome interrogando prima i servers della radice del dominio richiesto. Se il server DNS interrogato non può fornire la risposta finale, almeno fornisce al risolutore un record "NS" che rimanda il risolutore a un altro server DNS. Questo processo *iterativo* è ripetuto, e termina sicuramente quando il risolutore interroga l'*authoritative name server* (server dei nomi ufficiale) che è responsabile di un particolare dominio. Il DNS beneficia fortemente di un sistema di *caching*: molti *caching resolvers* mantengono una loro copia locale delle le informazioni richieste in precedenza, per migliorare le prestazioni: usano i dati dei records memorizzati per saltare alcune delle interazioni, o tutte, in modo da inviare l'informazione al cliente più velocemente.

L'uso dei forwarding resolvers nasconde l'indirizzo IP del cliente ai servers DNS ufficiali. Questo fornisce all'utente un certo livello di privacy impedendo agli operatori dei servers ufficiali di osservare l'origine delle richieste DNS. Naturalmente gli operatori dei forwarding resolvers possono ancora monitorare e censurare le richieste degli utenti, molto facilmente; inoltre i sistemi di monitoraggio passivi con sistemi come TURMOIL e XKEYSCORE possono anch'essi osservare qualsiasi parte della transazione sia disponibile al filtro di ingestione.

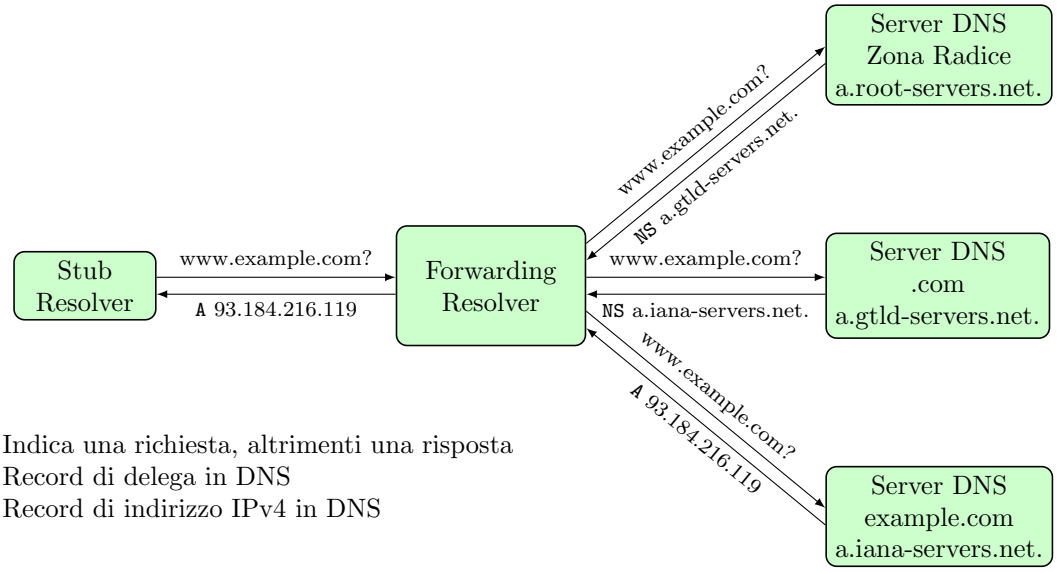



Figura 6: Risolvere il nome `www.example.com` con il DNS. Molti sistemi operativi forniscono solo degli *stub resolvers* minimali che inoltrano le richieste ai risolutori veri e propri. Per risolvere un nome questi risolutori cominciano interrogando i servers dei nomi della zona radice. Se un server non può fornire l'informazione richiesta rinvia il risolutore al prossimo server da interrogare, fino a che non si trova il server *ufficiale* per la rispettiva zona.

# 4 DNSSEC

In origine il sistema DNS non è stato progettato per fornire alcuna sicurezza, quando usato su una rete non sicura. Le Domain Name System Security Extensions (DNSSEC, estensioni di sicurezza per il DNS) aggiungono protezione d'integrità e autenticazione dell'origine dei dati ai records DNS. Comunque, poiché DNSSEC non aggiunge confidenzialità o protezione dal denial-of-service, non protegge minimamente dalla sorveglianza passiva. DNSSEC aggiunge dei tipi di records per le chiavi pubbliche ("DNSKEY"), delega del firmatario ("DS"), e per le firme sui records di risorsa ("RRSIG"). La figura 7 illustra le interazioni tra risolutori usando DNSSEC. DNSSEC crea un'infrastruttura a chiave pubblica gerarchica a cui tutti gli operatori DNSSEC debbono partecipare. Stabilisce una catena di fiducia dal server ufficiale di una zona fino al *trust anchor*, associato alla zona radice. Questa associazione si ottiene distribuendo la chiave pubblica della zona radice *fuori banda*, per esempio includendola nei sistemi operativi. Le catene di fiducia stabilite da DNSSEC rispecchiano la delega tra zone nel DNS. Con gli operatori di TLD tipicamente soggetti alla stessa giurisdizione degli operatori di dominio nella loro zona, queste catene di fiducia sono a rischio di attacchi attraverso mezzi sia tecnici che legali.

Segue una lista di alcune delle debolezze più gravi esibite dal DNS anche in presenza delle estensioni di sicurezza DNSSEC. DNSSEC non fornisce alcuna forma di privacy nelle risoluzioni di nomi da parte dell'utente: il contenuto di richieste e risposte DNS può essere spiato da qualsiasi avversario con accesso al canale di comunicazione e poi correlato con gli utenti, specialmente se l'avversario può osservare la connessione tra lo stub resolver e il forward resolver dell'utente. A livello tecnico, DNSSEC come messo in opera attualmente risente dell'uso del sistema di cifratura RSA (la zona radice usa RSA-1024), standard il cui supporto viene richiesto a ogni risolutore DNSSEC e che porta a chiavi di grandi dimensioni, un problema importante visto che ogni risposta include le firme per *tutti* gli schemi di firma supportati dal server ufficiale. Questo può portare a messaggi che superano la dimensione massima dei pacchetti DNS, il che causa altre vulnerabilità [7]. Infine, DNSSEC non è concepito per resistere ad attacchi *legali*. A seconda della loro influenza i governi, le imprese e le loro lobbies possono obbligare legalmente gli operatori dei DNS ufficiali a manipolare i dati, certificando i cambiamenti. Questo è particolarmente rilevante poiché DNSSEC mantiene la struttura gerarchica del DNS, dando quindi "fiducia" alla zona radice e agli operatori TLD in modo estensivo.

DNSSEC elimina inoltre le poche limitazioni tradizionali sull'acquisizione in massa di dati sulle zone, come ad esempio le restrizioni sui trasferimenti di zona. Prima di DNSSEC gli amministratori dell zone DNS potevano impedire i trasferimenti di zona, impedendo agli avversari di enumerare sistematicamente tutti i records DNS in una zona in modo semplice. Comunque, visto che il DNS consente risposte negative (NXDOMAIN), DNSSEC aveva bisogno di un modo di creare una dichiarazione firmata della non-esistenza di un record. Nell'ottica di mantenere sempre offline la chiave usata per la firma, furono introdotti i records "NSEC" per certificare che un intero intervallo di nomi non sono in uso. Osservando i limiti di questi intervalli un avversario può rapidamente enumerare tutti i nomi in uso in una zona. Un tentativo di evitare questo con l'introduzione del records "NSEC3" fu mostrato fondamentalmente sbagliato ancora prima di essere impiegato in modo significativo. Come conseguenza di tutto questo con DNSSEC diventa ancora più facile per un avversario scoprire servizi e sistemi vulnerabili.

# 5 Minimizzazione delle richieste

Tra le discussioni recenti nella IETF su come migliorare la privacy nel DNS spicca una proposta per la cosiddetta *minimizzazione delle richieste* [5], che ha buone possibilità di essere adottata rapidamente in quanto non richiede modifiche nel protocollo DNS. La minimizzazione delle richieste migliorerebbe leggermente la privacy facendo sì che iforwarding resolvers non mandino più la richiesta intera ai servers DNS contattati in ogni passo della risoluzione. Invece ogni server DNS riceverebbe solo la *parte* del nome necessaria per eseguire la sua parte del processo di risoluzione (Figura 8). Di conseguenza il nome richiesto sarebbe esposto nella sua interezza soltanto al server ufficiale finale.

La minimizzazione delle richieste si può implementare facilmente, cambiando il modo in cui i forwarding resolvers costruiscono le loro richieste iterative. La mininizzazione delle richieste avrebbe un impatto negativo sul caching, visto che almeno in teoria un server DNS può rispondere a una richiesta completa direttamente con la risposta finale — a causa di informazioni in cache, o quando il server è ufficiale per il nome completo in questione. Anche con la

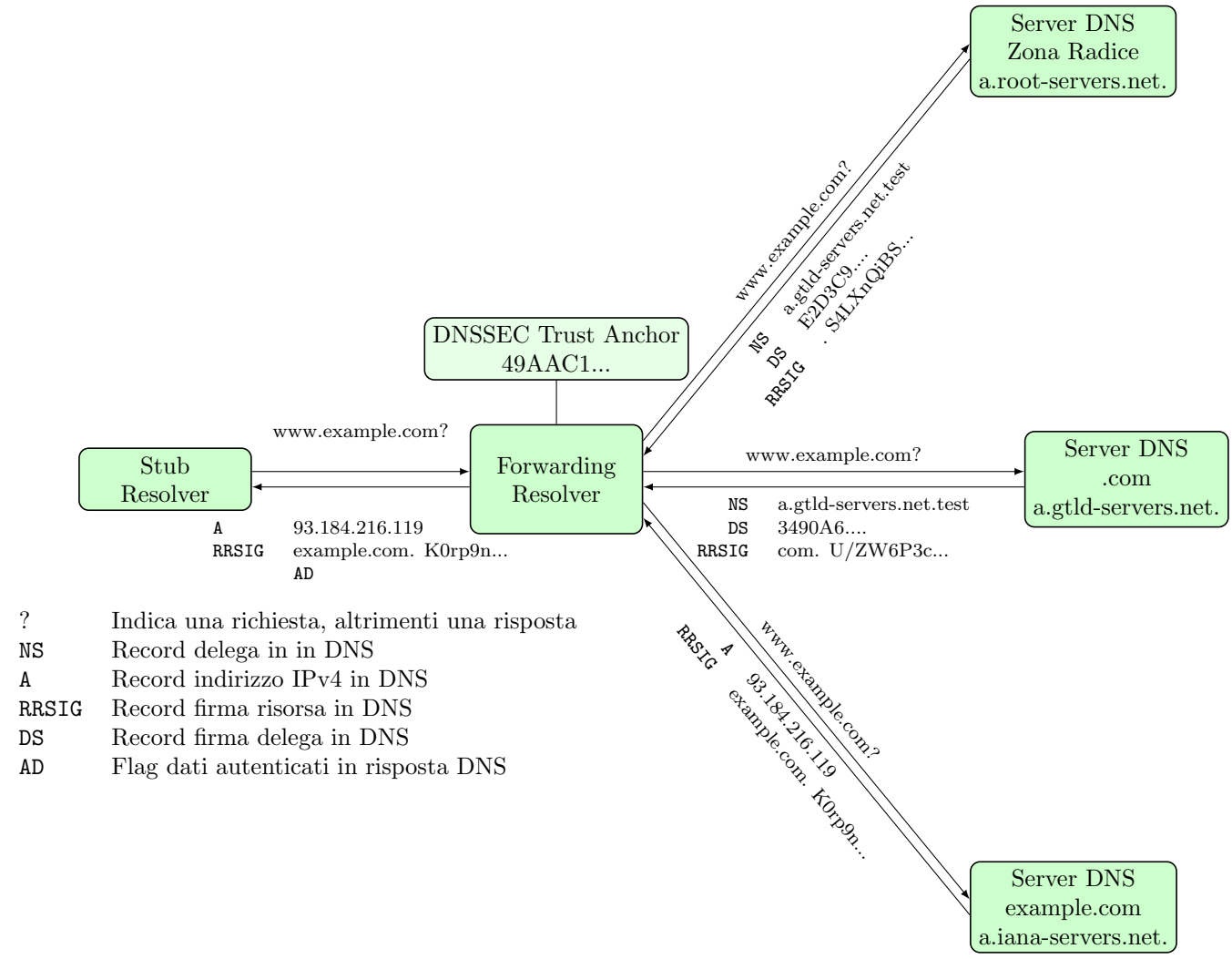



Figura 7: Risoluzione del nome `www.example.com` con DNS e DNSSEC: le informazioni inviate dal server sono firmate crittograficamente per assicurarne autenticità e integrità; le firme sono contenute nei records "RRSIG", e le informazioni sulla zona a livello superiore nei records "DS". Un risolutore può verificare una firma seguendo questa catena di fiducia e usando il *trust anchor* fornito fuori banda. Gli stub resolvers non possono verificare questa catena per conto proprio, ed è quindi il risolutore a indicare loro di aver verificato l'autenticità, attraverso il bit `AD` nella risposta da passare al cliente.

minimizzazione delle richieste i forward resolvers averbbero comunque accesso alla richiesta completa, e alla risposta per l'utente.

La minimizzazione delle richieste ha il vantaggio di richiedere modifiche solo ai forward resolvers, e lo svantaggio di mettere questo ipotetico cambiamento del tutto fuori dal loro controllo. La minimizzazione delle richieste si può combinare con vari approcci per cifrare il traffico DNS, presentati nelle prossime sezioni; senza la minimizzazione delle richieste la semplice cifratura del traffico DNS continua a esporre l'intera richiesta a molti servers DNS. Infine Verisign Inc. potrebbe impedire l'adozione delle minimizzazione delle richieste sfruttando il racket dei brevetti sul software [8].

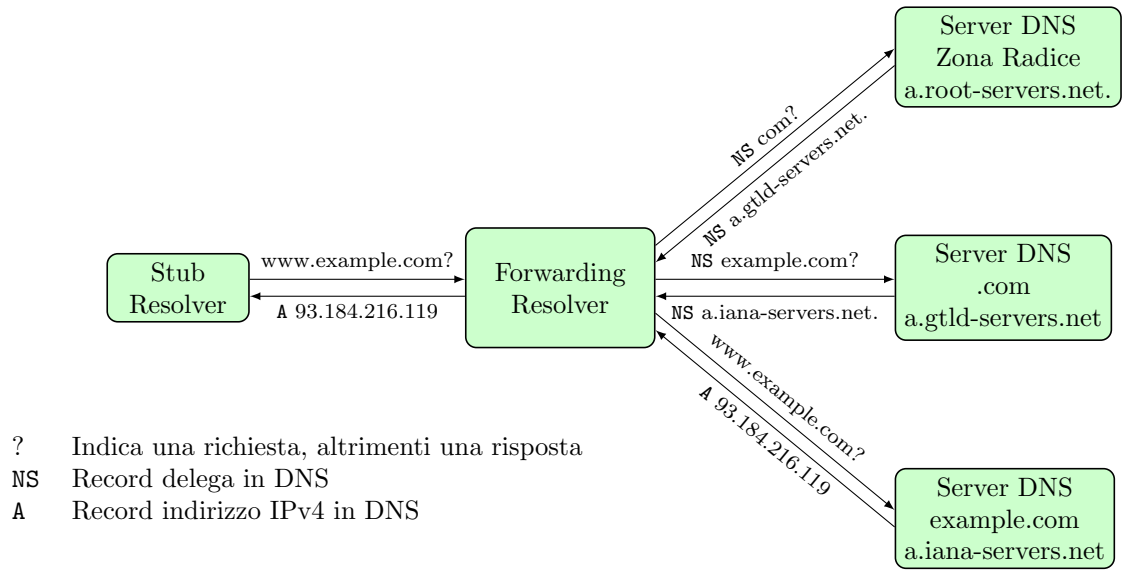



Figura 8: Con la minimizzazione delle richieste la risoluzione del nome `www.example.com` non espone più il nome completo e il tipo di query alla zona radice e all'autorita `.com`; anche in questo schema rimangono comunque informazioni sensibili che filtrano fino al server DNS del TLD. Inoltre l'effetto è ancora più debole in pratica, visto che la zona radice viene contattata di rado già col sistema attuale, grazie al caching d'informazioni al livello dei forwarding resolvers.

# 6 T-DNS: DNS sopra TLS

L'idea di usre TLS per cifrare il traffico DNS è stata spesso rifiutata in passato a causa della perdita di prestazioni associata. Comunque in una bozza recente della IETF gli autori fanno notare i benefici di far passare DNS su TLS non solo in termini di privacy: passare da UDP a TCP (quindi a un protocollo orientato alle connessioni) potrebbe mitigare gli attacchi di amplificazione sui (o anche *dai*) servers DNS [9].

Ri-usando una connessione TCP per richieste DNS multiple con dei *timeouts ragionevoli*, le richieste in *pipeline* e permettendo un'elaborazione *fuori ordine*, la proposta T-DNS promette prestazioni ragionevoli malgrado l'overhead di TCP e TLS.

Comunque, anche se TLS fosse adottato per il DNS, i metadati filtrerebbero ancora all'esterno permettendo a terzi di determinare i dati DNS richiesti da un utente: nella proposta della IETF si combina TLS con l'uso dei forward resolvers, che se da un lato nascondono l'indirizzo IP dell'utente ai servers DNS, dall'altro hanno ancora il potere di spiare l'utente essi stessi. Inoltre TLS stesso non ha una storia particolarmente positiva con dozzine di problemi riportati negli ultimi anni, da compromissioni di alto profilo nelle autorità di certificazione a difetti d'implementazione e modalità di cifratura insicure.

TLS non è l'unico metodo possibile per cifrare le richieste e risposte DNS in rete. DNSCurve e Confidential DNS sono proposte alternative per proteggere il contenuto di richieste e risposte dal monitoraggio a livello di rete.

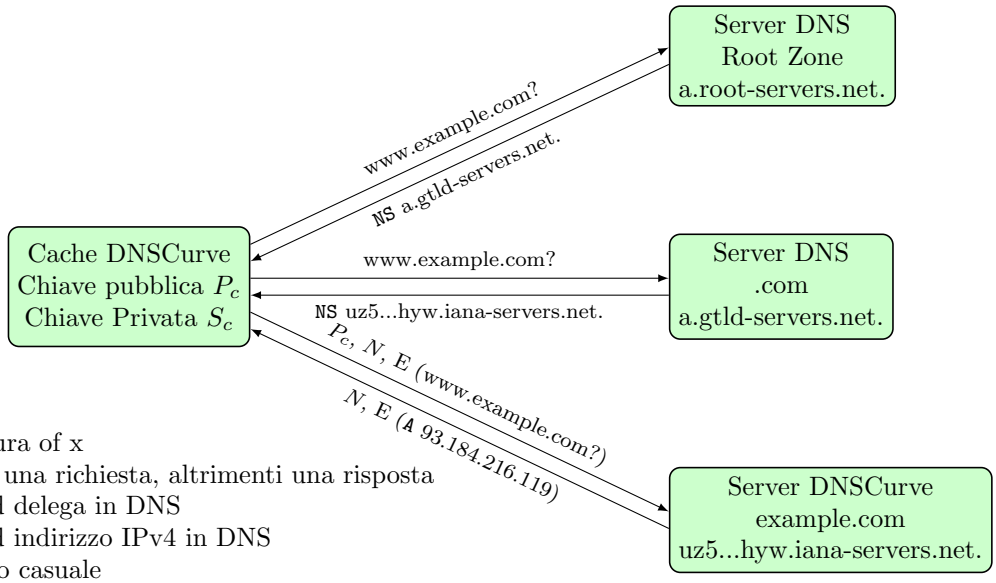
# 7 DNSCurve

Il primo sistema pratico per migliorare la confidenzialità di richieste e risposte DNS è stato DNSCurve [6]. In DNSCurve prima ci si scambiano delle chiavi di sessione usando Curve25519 [1], e poi le si usano per fornire autenticazione e cifratura tra caches e servers. DNSCurve migliora il sistema DNS esistente fornendo confidenzialità e integrità senza bisogno di generare firme in modo costoso o sessioni (D)TLS. Specificamente DNSCurve raggiunge lo stesso Round Trip Time (RTT, tempo di andata e ritorno) del DNS attuale incorporando la chiave pubblica del server nel record "NS".

DNSCurve crea un'associazione autenticata e cifrata tra un *server DNSCurve* e una *cache DNSCurve*, ossia un risolutore DNS ricorsivo con caching che gira su un endpoint al posto di un risolutore stub (Figura 9). Non essendo previste firme una cache DNSCurve non può provare l'autenticità dei records in cache ad altri utenti, limitando l'utilità di ogni cache al suo rispettivo endpoint.

Anche se in DNSCurve l'utente non ha più bisogno di fidarsi di un forward resolver, l'indirizzo IP dell'endpoint è ora esposto ai servers DNS ufficiali: non è più oscurato dai forward resolvers gestiti dagli ISP. Di conseguenza DNSCurve può migliorare la privacy contro un avversario che osserva il traffico DNS su sistemi intermedi o ascoltando sui cavi, ma al contempo *riduce* la privacy nei confronti dei servers DNS ufficiali, esposti sia alla richiesta completa che all'identità (indirizzo IP) dell'utente. Un altro difetto noto di DNSCurve è la necessità di mantenere online le chiavi private. DNSCurve inoltre non può proteggere dalla censura, visto che alcuni governi continuano tuttora a controllare la gerarchia dei *registrars*, e possono quindi far scomparire interi domini. Parlando degli attacchi della NSA, DNSCurve difende gli utenti solo dalla sorveglianza passiva sul cavo, proteggendo la confidenzialità almeno del contenuto di richieste e risposte.

Anche con DNSCurve i servers DNS rimangono un obiettivo succoso per la sorveglianza di massa. Inoltre, come con DNS, i servers DNS noti e facili da localizzare rimangono un bersaglio e un vettore di conferma per attacchi a infrastruttura critica. Con DNSCurve il bisogno di crittografia a chiave pubblica online da parte delle autorità DNS può aprire un'altra vulnerabilità agli attacchi *Denial of Service* quando si usa una CPU "lenta" per gestire un collegamento "veloce".




| | |
|---|---|
| E(x) | Cifratura of x |
| ? | Indica una richiesta, altrimenti una risposta |
| `NS` | Record delega in DNS |
| `A` | Record indirizzo IPv4 in DNS |
| $N$ | numero casuale |
| $S_c/P_c$ | Chiave Segreta/Pubblica della cache |

Figura 9: Risoluzione del nome `www.example.com` con DNSCurve. Con DNSCurve la cache di risoluzione e il server DNSCurve si scambiano un messaggio segreto condiviso per cifrare la loro comunicazione. La chiave pubblica del server DNSCurve è codificata in nome del name server stesso usando Base32. Quando una cache DNSCurve risolve un nome e scopre che il server supporta DNSCurve la cache crea un messaggio segreto condiviso basato sulla chiave pubblica del server, la chiave privata della cache, e un numero casuale usato una sola volta. La cache invia la sua chiave pubblica, il numero e la richiesta cifrata col messaggio segreto condiviso. Il server risponderà con il risultato della richiesta cifrato col messaggio segreto condiviso. Le prime due richieste alla zona radice e al TLD "`.com`" non usano DNSCurve nell'illustrazione, visto che attualmente i servers in questione non lo supportano.

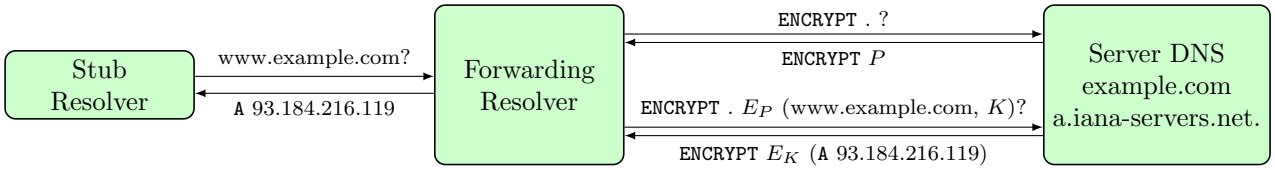
### DNSCrypt

DNSCrypt è un protocollo non standardizzato ma documentato, largamente basato su DNSCurve. Protegge le richieste del risolutore stub dell'utente finale dalla sorveglianza sulla rete e dalle modifiche. Poiché è basato su DNSCurve nemmeno DNSCrypt risolve i problemi più importanti di privacy e sicurezza presenti nel DNS. Il risolutore conosciuto più grande che supporta DNSCrypt è OpenDNS. Esiste un certo numero di risolutori DNSCrypt gestiti dalla comunità DNSCrypt. Ad oggi DNSCrypt rimane il protocollo di cifratura DNS più usato per impedire la sorveglianza degli utenti finali in rete. Purtroppo risolve il problema della privacy solo per metà, e non è largamente adottato o standardizzato.

## 8 Confidential DNS

Un'altra bozza recente della IETF suggerisce un metodo alternativo per un DNS cifrato, basato proprio sul meccanismo di estensione principale di DNS, l'introduzione di nuovi tipi di records [19]. Confidential DNS introduce un nuovo tipo di record "ENCRYPT" che fornisce una chiave pubblica necessaria al risolutore ricorsivo per cifrare la connessione con il server DNS. Questo record "ENCRYPT" contiene la chiave pubblica del server DNS da usare per cifrare la comunicazione iniziata dal risolutore, evitando la soluzione sporca di DNSCurve che aggiunge la chiave pubblica alla risposta "NS" della zona che delega.

La bozza attuale supporta due diverse modalità operative: una modalità *opportunistica*, più semplice da realizzare in quanto non richiede modifiche importanti all'infrastruttura DNS, e un modalità *autenticata*, in cui le chiavi pubbliche di un dominio sono memorizzate anche nella rispettiva zona di livello superiore, il che ovviamente richiede supporto nell'infrastruttura DNS della zona superiore.




| | |
|---|---|
| ? | Indica una richiesta, altrimenti risposta |
| . | Richiesta per la zona radice |
| $P$ | Chiave pubblica del server |
| $K$ | Chiave di cifratura |
| $E_P$ (x) | Cifratura di of x con $P$ |
| $E_K$ (x) | Cifratura x con $K$ |
| `A` | Record indirizzo IPv4 in DNS |
| `ENCRYPT` | Record ENCRYPT in DNS |

Figura 10: Risoluzione del nome `www.example.com` con Confidential DNS opportunistico. Il risolutore ottiene la chiave pubblica del server DNS richiedendo il nuovo record "ENCRYPT", e successivamente usa la chiave pubblica per cifrare la richiesta al server. Il risolutore invia la richiesta cifrata con la chiave pubblica del server, e la chiave con cui cifrare la risposta.

In modalità opportunistica la chiave pubblica non è più associata alla zona di livello superiore ed è invece servita separatamente in chiaro e possibilmente senza autenticazione, come un record di zona. Di conseguenza Confidential DNS con il record "ENCRYPT" supporta solo la cosiddetta *cifratura opportunistica* — un modo attraente per dire che *la cifratura si può scavalcare banalmente* con un attacco man-in-the-middle, visto che le chiavi usate per la cifratura non sono autenticate.

L'uso di nuovi tipi di records crea anche l'opportunità per la complessità "tipica" dei progetti ingegneristici definiti da commissioni: Confidential DNS può usare crittografia simmetrica o asimmetrica, può supportare RSA a

512 bits e AES in modalità CBC (utilizzato recentemente per uccidere finalmente SSL3 [10]). La bozza non stabilisce un supporto minimo sufficientemente forte, e non prevede che questo minimo possa essere aggiornato in futuro in risposta a nuove considerazioni sulla sicurezza.

La bozza su Confidential DNS fornisce un secondo metodo per ottenere una "vera" cifratura autenticata memorizzando la chiave pubblica di un dominio nella rispettiva zona di livello superiore. Per ottenere questo Confidential DNS estende i records Delegation Signer ("DS") di DNSSEC in modo sporco per fornire la chiave di cifratura per la zona, più o meno come DNSCurve estende i records "NS". La bozza prevede diverse modalità di fallimento come "fallback to insecure", che permette ai clienti di adottare connessioni insicure "sperando che tutto vada bene", anche *dopo* l'individuazione di una connessione sicura. A causa di questo comportamento "fallback to insecure", adottato anche in caso di algoritmi crittografici non supportati, Confidential DNS fornisce un *livello di sicurezza imprevedibile*, invece di qualsiasi tipo di garanzia. Non offrire garanzie e fornire molte opzioni facilita la messa in opera e la migrazione, che è il principio-guida per il processo ingegneristico guidato dall'industria della IETF.

Confidential DNS è disponibile nei servers DNS Unbound dal 2011.

# 9 Namecoin

Alcuni sistemi peer-to-peer alternativi forniscono soluzioni più radicali al problema della risoluzione dei nomi sicura. Sono stati proposti sistemi basati su timelines alla maniera di Bitcoin [11] per creare un sistema di nomi globale e sicuro [15]. Qui l'idea è creare una singola timeline delle registrazioni dei nomi accessibile globalmente, a cui si possa solo aggiungere in coda. I sistemi basati su timeline dipendono da una rete peer-to-peer per gestire gli aggiornamenti e memorizzare la timeline stessa. Nel sistem Namecoin [16] le modifiche alle coppie chiave-valore vengono incluse nelle transazioni da aggiungere alla timeline per mezzo del *mining*. Il mining è l'uso di metodi a forza bruta per cercare delle collisioni hash (parziali) con una fingerprint che rappresenti lo stato completo globale — compresa l'intera storia dei cambiamenti — della timeline.

Date due timelines con delle coppie chiave-valore potenzialmente in conflitto, la rete accetta come valida la timeline con la catena più lunga, in quanto essa corrisponde a una quantità di potenza computazionale spesa maggiore. L'idea è di impedire agli avversari di creare delle timelines alternative rendendolo computazionalmente troppo costoso. Questo assume una potenza di calcolo limitata, il che potrebbe non applicarsi in pratica ad alcuni avversari.

Per eseguire una richiesta di un nome con Namecoin il cliente deve controllare se la timeline contiene una entry per il nome desiderato, e verificare la correttezza della timeline. Per fare questo l'utente deve possedere una copia completa della timeline, la cui dimensione era di 2GB nel novembre 2014[3]; alternativamente gli utenti possono usare un server di nomi di cui si fidino, che partecipi nella rete Namecoin.

Namecoin può migliorare la privacy dell'utente se la catena dei blocchi completa è replicata sul sistema locale dell'utente. In questo caso la risoluzione di un nome non implica una richiesta, ed è quindi completamente privata. Comunque replicare la catena completa dei blocchi per ogni utente potrebbe diventare poco pratico su alcuni apparecchi, nel caso in cui Namecoin crescesse e diventasse un concorrente serio del DNS attuale. Namecoin inoltre non evita lo spionaggio sulle informazioni delle zone; in particolare enumerare le zone è banale. Comunque la natura decentralizzata di Namecoin assicura che almeno "l'indicazione dei danni di battaglia" contro un server di nomi non abbia più senso.

# 10 GNS: il sistema di nomi GNU

Gli autori di questo articolo stanno lavorando allo GNU Name System (sistema di nomi GNU, GNS) [17], una proposta più radicale per risolvere i problemi di privacy e sicurezza del DNS, che come Namecoin si allontana notevolmente dal processo di risoluzione del DNS. Il processo di risoluzione di GNS non fa usao di risolutori che interrogano delle autorità DNS. GNS usa invece una rete peer-to-peer a una tabella hash distribuita (Distributed Hash Table, DHT) perché i risolutori possano trovare delle associazioni chiave-valore.

[3] `https://bitinfocharts.com/de/namecoin/`

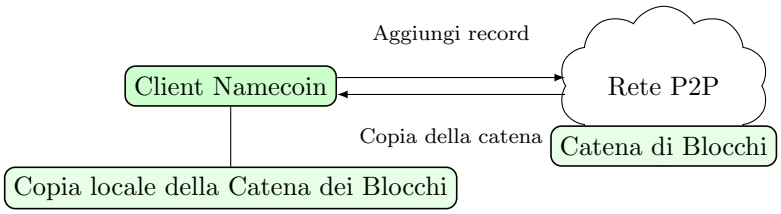



Figura 11: Il sistema di nomi Namecoin è decentralizzato e usa una rete peer-to-peer. Per ottenere un consenso sui nomi registrati Namecoin adotta una *catena di nomi* memorizzata nella rete peer-to-peer. Per registrare i nomi i clienti devono eseguire del lavoro computazionale prima di poter aggiungere un nome in fondo alla catena. Per risolvere un nome i clienti devono possedere una copia completa della catena dei blocchi, e cercare al suo interno il nome da risolvere.

GNS preserva la privacy visto che le richieste e le risposte sono cifrate, e anche un avversario che partecipasse attivamente potrebbe nel caso peggiore eseguire un "attacco di conferma" e apprendere quindi solo il tempo di scadenza di una risposta. È importante notare che sono le stesse richieste e risposte a essere cifrate, e non le connessioni tra un risolutore e una qualche autorità. Poiché tutte le risposte sono non solo cifrate ma anche firmate crittograficamente, i peers nella DHT non possono falsificare i risultati senza essere immediatamente individuati.

Attraverso l'uso della DHT, GNS evita certe complicazioni del DNS come i "records colla" e le interrogazioni a server di dominio fuori dal loro dominio (out-of-bailiwick lookups). In GNS le etichette di un nome corrispondono esattamente alla sequenza delle interrogazioni, rendendo il cammino di fiducia completo perfettamente ovvio per l'utilizzatore. Infine l'uso di una DHT per distribuire i records permette anche alle autorità GNS di gestire delle zone senza un'infrastruttura critica che sia visibile o associabile a qualcuno, da poter usare per la stima dei danni di battaglia.

GNS può risolvere i nomi in modo sicuro associando oggetti qualsiasi. Può quindi essere usato per l'indirizzamento, la gestione di identità e come alternativa alle complicate infrastrutture a chiave pubblica di oggi.

## 10.1 Nomi, zone e deleghe

Una zona GNS è una coppia di chiavi pubblica-privata con un insieme di record associati. Il processo di risoluzione dei nomi in GNS essenzialmente risolve una catena di chiavi pubbliche. In assenza di una *zona radice* largamente usata e riconosciuta, ma anche come un'alternativa intenzionale all'indirizzamento gerarchico, GNS usa lo pseudo-TLD "`.gnu`" per riferire alla zona di ciascun utente detta `zona principale`. Ogni utente può creare un numero arbitrario di zone, ma una deve essere designata come la principale. Gli utenti possono gestire liberamente le associazioni per le etichette all'interno delle loro zone. Possono anche, e questo è il punto importante, delegare il cotnrollo su un sotto-dominio a qualsiasi altra zona (comprese quelle gestite da altri utenti) usando un record "PKEY", che semplicemente specifica il cammino di deleghe menzionato più in alto. Grazie alla DHT non è necessario specificare l'indirizzo di un qualche sistema responsabile di gestire la zona delegata. La validità dei records nella DHT è stabilita usando firme e crittografiche e verificandone la scadenza.

## 10.2 Crittografia per la privacy

Per permettere ad altri utenti di ricercare i records di una zona, tutti i records per una data etichetta sono memorizzati nella DHT in un blocco firmato crittograficamente. Al fine di massimizzare la privacy degli utenti nella consultazione della DHT sia le richieste che le risposte sono cifrate usando una chiave pubblica derivata dalla chiave pubblica della zone e dall'etichetta. Un peer può facilmente validare la firma ma non decifrare la risposta senza una conoscenza a priori della chiave pubblica e dell'etichetta della zona. Di conseguenza gli utenti possono usare delle passwords come etichette, o usare delle chiavi pubbliche non note pubblicamente per restringere intenzionalmente l'accesso all'informazione sulle zone. Grazie alla DHT, tutte le interrogazioni GNS sono dirette alla stessa infrastruttura globale decentralizzata invece che a dei servers specifici a un operatore. Questo rende impossibile la compromissione di un server specifico a una zona, visto che tutte le macchine che realizzano la DHT

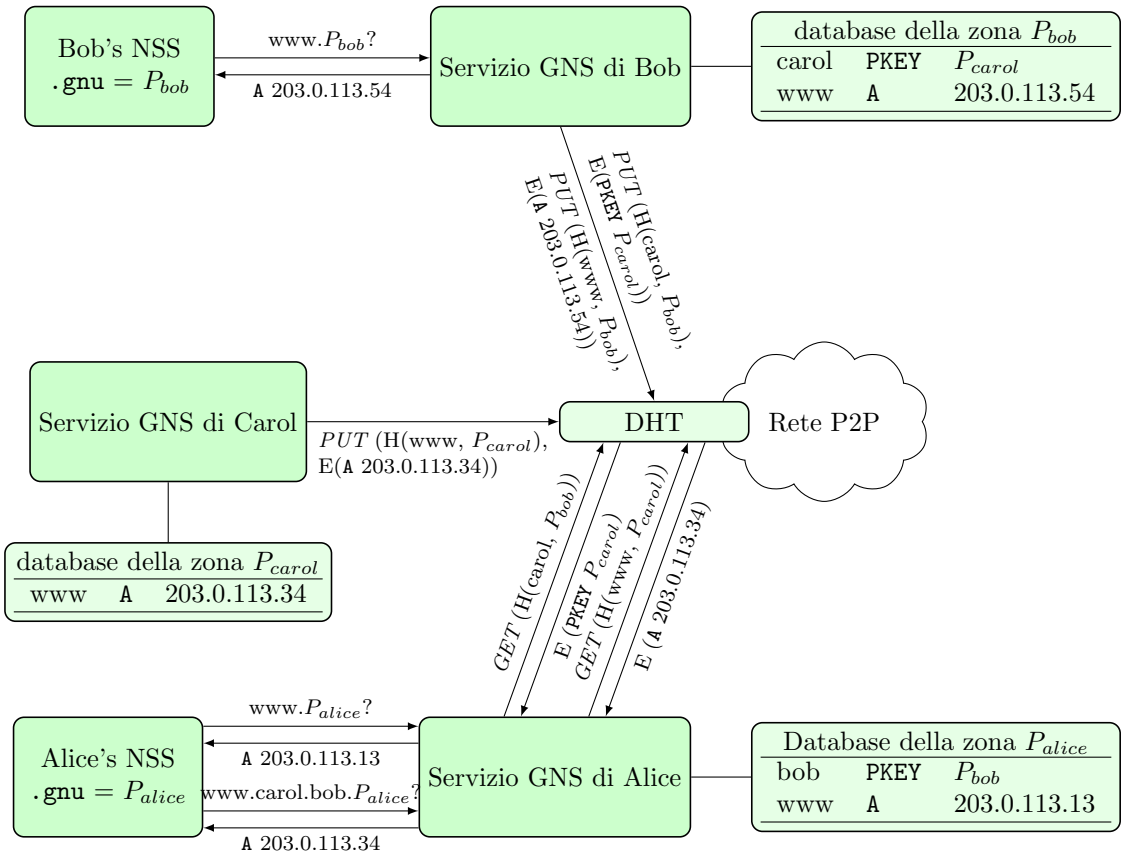



Figura 12: Il sistema di nomi GNU: con GNS ogni utente mantiene il suo database contenente degli insiemi di records associati a etichette organizzate in zone. Una zona si riferisce a una coppia di chiavi pubblica-privata. Qui Alice, Bob e Carol hanno dei servers web tutti e tre raggiungibili sotto il nome `www.gnu.org`. Per Alice `www.gnu.org` si risolve a un indirizzo diverso rispetto a quelli di Bob e Carol, visto che i loro rispettivi commutatori del servizio di nomi (Name Service Switches, NSS) locali associano a `.gnu` una chiave pubblica specifica all'utente. Per permettere agli altri utenti di risolvere i nomi, l'informazione sulla zona pubblica di un utente è cifrata e pubblicata in una DHT sotto un nome di chiave offuscato. Un utente può risolvere nomi *delegando* al namespace di un altro utente che si trova nel suo namespace. Alice può accedere al namespace di Bob delegando il controllo sul nome `bob` a $P_{bob}$ nel suo namespace, usando un record "PKEY" specifico a GNS. In questo modo Alice può accedere al server web di Carol usando il nome `www.carol.bob.gnu`.

sono repsonsabili, congiuntamente, di tutte le zone — le coppie chiave-valore non rivelano neppure a quale zona appartengono. Allo stesso tempo la cifratura e l'autenticazione dei records è critica per proteggere gli utenti dalla censura e dalla sorveglianza. Comunque, diversamente dalle altre proposte meno radicali per migliorare il DNS, mettere in opera GNS sarà una sfida significativa: GNS richiede dei cambiamenti al software più significativi, oltre a uno sforzo da parte della comunità per realizzare una DHT come una nuova infrastruttura pubblica.

# 11 Sviluppi politici

Il sistema di gestione dei nomi e il registro degli indirizzi IP di IANA solo i due databases importanti che legano insieme l'Internet globale. Dato lo sfruttamento spudorato di Internet come una macchina per la sorveglianza da parte del suo gestore attuale, il governo statunitense, il trend verso delle "Internet nazionali" rischia di accelerare ulteriormente.

Alcuni paesi, particolarmente quello che censurano Internet in modo più pesante come Cina e Iran, hanno chiuso la loro Internet nazionale al fine di limitare il flusso d'informazioni per qualche tempo. Comunque, particolarmente dopo le rivelazioni di Snowden, i dibattiti sul routing tra nazioni e la costruzione di infrastrutture nazionali si sono accesi anche in paesi considerati tradizionalmente alleati fidati degli USA: in Brasile si è parlato di obbligare le grandi piattaforme Internet a stabilire una presenza nel paese, e a mantenere i dati brasiliani fisicamente in Brasile. In Germania ci sono state richieste di routing ristretto alla nazione o a Schengen. La diminuzione d'importanza della funzione della IANA, richiesta fin dalla prima conferenza dell'ONU sulla Società dell Informazione (World Summit of the Information Society), è stata finalmente annunciata dalla NTIA ad Aprile.

Come al solito le agenzie di spionaggio hanno cominciato in anticipo a isolarsi: sia la NSA che il GCHQ operano un servizio DNS non pubblico con i loro TLD non ufficiali, `.nsa` e `.gchq`. (Comunque, diversamente dagli sviluppatori di Tor, le agenzie di spionaggio non hanno ancora seguito l'RFC 6761 per riservare questi nomi.)

L'uso strategico di TLD non pubblici per rendere i servizi Internet meno accessibili è logico, ed è un passo chiaro verso la "balcanizzazione" di Internet. A una scala globale questo trend non è apprezzato dal governo statunitense, poiché la decentralizzazione può limitare il raggio d'azione della sorveglianza USA. Al fine di evitare questo sviluppo un processo "plurale" viene usato per oscurare la questione di *chi* opera il sistema, e per evitare il problema della responsabilità mantenendo allo stesso tempo un controllo indiretto tramite i "portatori d'interesse".

Negl ultimi anni la ICANN ha tentato di aumentare la competizione nelle offerte dei nomi di dominio, con la proliferazione dei GTLD; rimane comunque un'organizzazione incorporata negli USA a controllare processi e profitti. Una domanda chiave quindi è se sarà ICANN/IANA o qualche successore, sotto una qualche struttura di governance, a dirigere la situazione. Un'alternativa è lo sviluppo e la messa in opera di tecnologie che decentralizzano completamente l'allocazione di indirizzi e nomi, rendendo inutile un gestore globale e tutte le lotte politiche per il suo controllo. Sembra che Internet si stia muovendo in tutte e due le direzioni allo stesso tempo.

# 12 Conclusione

In "La cultura è il nostro business" Marshall McLuhan ha affermato profeticamente:

> "La Terza Guerra Mondiale è una guerriglia per le informazioni senza divisione tra partecipazione civile e militare."

Questa previsione che risale agli anni 1970 sembra rimanere rilevante oggi, considerando l'architettura di Internet per come è tessuta attraverso le nostre vite di ogni giorno.

Il DNS non è stato mai progettato con la privacy o la sicurezza come obiettivi. Nella battagli degli stati-nazione per il dominio globale qualsiasi infrastruttura di Internet che serva un pubblico specifico diventa un bersaglio per stati ostili. L'infrastruttura critica deve essere decentralizzata logisticamente e dovrebbe idealmente essere condivisa a livello globale, per disincentivare il suo danneggiamento. Semplicemente cifrare il traffico DNS e web può non essere abbastanza per ridurre l'effetto di attacchi mirati contro architetture insicure.

Mentre nella comunità DNS esiste la consapevolezza che la privacy è un problema, i vari interessi in conflitto nella comunità rendono praticamente impossibile un qualche progresso significativo per consenso. Le proposte di modifica a sistemi già in opera come il DNS, in seguito a un trend generale di fossilizzazione di Internet, sono trattate con inerzia e tendono a morire soffocate dalle commissioni, come se qualsiasi cambiamento significativo potesse provocare non solo malfunzionamenti, ma anche avere impatto sul modello di business di qualcuno, o sull'interesse di stati-nazione.

In un mondo in cui la NSA dà la caccia agli amministratori di sistema[4] a la ICANN diventa una facile vittima[5], le toppe proposti dalla IETF sono insufficienti rispetto alla dimensione del problema: la sorveglianza degli utenti, la censura commerciale e il pericolo di un nuovo regno di terrore ove gli operatori del DNS siano obiettivi legittimi; tutto questo deve essere tenuto in conto nei progetti futuri.

[4] `http://cryptome.org/2014/03/nsa-hunt-sysadmins.pdf`

[5] `http://www.heise.de/security/meldung/Erfolgreicher-Angriff-auf-Internet-Verwaltung-ICANN-2499609.html`

### Ringraziamenti

Desideriamo ringraziare Laura Poitras, Ludovic Courtès, Dan Bernstein, Luca Saiu e Hellekin Wolf per il loro aiuto e supporto nella preparazione di questo rapporto.

## Riferimenti bibliografici

[1] Daniel J. Bernstein. Curve25519: new Diffie-Hellman speed records. In *In Public Key Cryptography (PKC), Springer-Verlag LNCS 3958*, 2006.

[2] Internet Architecture Board. IAB Statement on Internet Confidentiality. `https://mailarchive.ietf.org/arch/msg/ietf-announce/ObCNmWcsFPNTIdMX5fmbuJoKFR8`, November 2014.

[3] S. Bortzmeyer. Possible solutions to DNS privacy issues. `http://tools.ietf.org/html/draft-bortzmeyer-dnsop-privacy-sol-00`, Dec 2013.

[4] S. Bortzmeyer. DNS privacy considerations. `https://datatracker.ietf.org/doc/draft-ietf-dprive-problem-statement/`, October 2014.

[5] S. Bortzmeyer. DNS query name minimisation to improve privacy. `https://tools.ietf.org/html/draft-bortzmeyer-dns-qname-minimisation-02`, May 2014.

[6] D. J. Bernstein. DNSCurve: Usable Security for DNS. `http://dnscurve.org/`, August 2008.

[7] Amir Herzberg and Haya Shulman. Fragmentation Considered Poisonous: or one-domain-to-rule-them-all.org. In *CNS 2013. The Conference on Communications and Network Security. IEEE*. IEEE, 2013.

[8] Verisign Inc. Verisign Inc.'s Statement about IPR related to draft-bortzmeyer-dns-qname-minimisation-02. `https://datatracker.ietf.org/ipr/2469/`, Oct 2014.

[9] Allison Mankin, Duane Wessels, John Heidemann, Liang Zhu, and Zi Hu. t-DNS: DNS over TCP/TLS. `http://www.isi.edu/ant/tdns/`, December 2014.

[10] Bodo Möller, Thai Duong, and Krzysztof Kotowicz. This POODLE bites: exploiting the SSL 3.0 fallback. `https://www.openssl.org/~bodo/ssl-poodle.pdf`, September 2014.

[11] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. `http://bitcoin.org/bitcoin.pdf`, 2008.

[12] Anonymous (NSA). There is more than one way to quantum. `https://www.documentcloud.org/documents/1076891-there-is-more-than-one-way-to-quantum.html#document/p1`, March 2014.

[13] NSA/CSS Thread Operations Center (NTOC). Bad guys are everywhere, good guys are somewhere! `http://www.spiegel.de/media/media-34757.pdf`, September 2014.

[14] Redacted (NSA, S32X). QUANTUMTHEORY. `https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/`, March 2014.

[15] Aaron Swartz. Squaring the Triangle: Secure, Decentralized, Human-Readable Names. `http://www.aaronsw.com/weblog/squarezooko`, January 2011.

[16] `http://dot-bit.org/`. The Dot-BIT project, A decentralized, open DNS system based on the bitcoin technology. `http://dot-bit.org/`, April 2013.

[17] Matthias Wachs, Martin Schanzenbach, and Christian Grothoff. A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System. In *13th International Conference on Cryptology and Network Security (CANS 2014)*, pages 127–142, 2014.

[18] Nicholas Weaver. A Close Look at the NSA's Most Powerful Internet Attack Tool. *Wired*, 2014.

[19] W. Wijngaards. Confidential DNS. http://tools.ietf.org/html/draft-wijngaards-dnsop-confidentialdns-00, November 2013.