

Are we ready for nsec3-guidance?

13 June 2022

ICANN74 DNSSEC and Security Workshop
Yoshiro YONEYA <yoshiro.yoneya@jprs.co.jp>

Background (1/2)

- nsec3-guidance is going to be a BCP RFC soon
 - <https://datatracker.ietf.org/doc/draft-ietf-dnsop-nsec3-guidance/>
 - For more technical background, please refer to Viktor Dukhovni's talk at ICANN70 DNSSEC and Security Workshop
 - [NSEC3 Iterations etc. High Counts and opt-out considered harmful, avoid fixed salt](#)

Background (2/2)

- nsec3-guidance affects both zone publishers (authoritative DNS side) and DNSSEC validator operators (full resolver side), but timing of when they will follow nsec3-guidance may differ
- Due to the timing difference, possibility of name resolution failure of TLDs (large outages) is highly concerned

Objective of this talk

- Explain possibility of the large outages at TLDs and propose some mitigations
- **Aiming smooth deployment of nsec3-guidance**

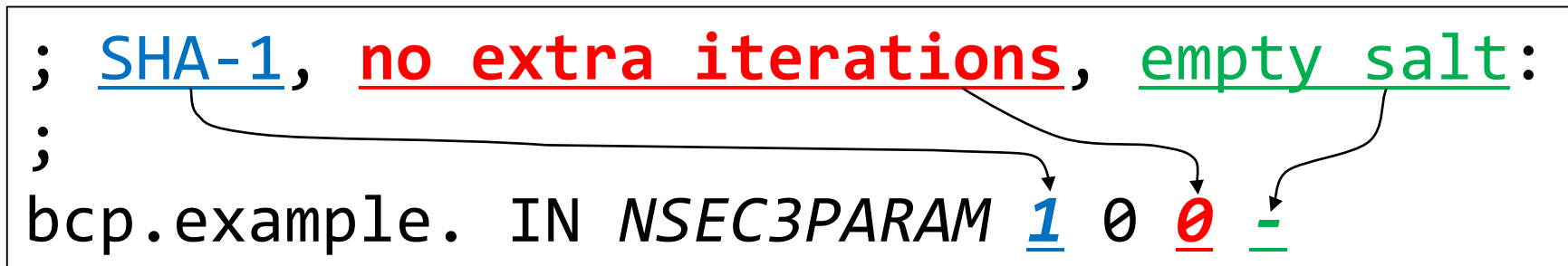
Key points of nsec3-guidance (1/3)

- Premise
 - nsec3-guidance indicates that using iteration count larger than 0 is less effective and possible security threat (can be a cause of DoS attack)

Key points of nsec3-guidance (2/3)

- Best-practice for Zone Publishers
 - If NSEC3 must be used, then an *iterations count of 0 MUST be used* to alleviate computational burdens
 - The *recommended NSEC3 parameters* are:

```
; SHA-1, no extra iterations, empty salt:  
;  
bcp.example. IN NSEC3PARAM 1 0 0 -
```



- The *use of opt-out based NSEC3 records is NOT RECOMMENDED* except for very large and sparsely signed zones

Key points of nsec3-guidance (3/3)

- Recommendation for Validating Resolvers
 - *Validating resolvers MAY return an insecure response* to their clients when processing *NSEC3 records with iterations larger than 0*
 - *Validating resolvers MAY also return a SERVFAIL response* when processing *NSEC3 records with iterations larger than 0*

Impacts to TLDs using NSEC3 (1/2)

- DNS name resolution of TLDs who using NSEC3 with iteration count larger than 0 may be resulted in insecure or SERVFAIL someday after the publication of nsec3-guidance BCP RFC
- Major DNS software/service developers are favorable to nsec3-guidance, therefore, default setting for DNSSEC validator will follow the BCP in the future

Impacts to TLDs using NSEC3 (2/2)

- Especially, when large public DNS resolver services started to follow BCP, TLDs not following the BCP will be possible to become unresolvable globally (fear of large outage!)
- If this happened, customer support of ISPs will be overflow by claims from the end users
- And therefore validator operators will put the TLDs in NTA permanently, THAT IS NEGATIVE PRACTICE FOR DNSSEC DEPLOYMENT
 - Recovery from this practice is very hard

How many TLDs will be affected?

| | | | | | | | | | | | | | | | | | | | | |
|----|-----|-----|-----|-----|------|------|-------|--|-------|---------|---------|---------|----------|-----------|------------|----------------|-----------------|------------|-----------|-----|
| AC | LV | AFL | GOT | ONL | ZIP | FREE | PING | ACTOR | LAMER | TOTAL | FLICKR | SCHULE | COMPANY | RENTALS | ETISALAT | HOMESENSE | PRODUCTIONS | 谷歌 | ישראל | |
| AD | LY | AIG | GOV | OOO | ABLE | FUND | PINK | ADULT | LEASE | TOURS | FUTBOL | SEARCH | COMPARE | REVIEWS | EXCHANGE | INSTITUTE | PROGRESSIVE | מוקד | موقع | |
| AF | MA | ANZ | HBO | ORG | ADAC | GBIZ | PLAY | AETNA | LEGAL | TRADE | GALLUP | SECURE | CONTACT | SAMSUNG | FEEDBACK | INSURANCE | REDUMBRELLA | 電訊盈科 | عمان | |
| AG | MC | APP | HIV | OTT | AERO | GENT | PLUS | AMICA | LEXUS | TUNES | GARDEN | SELECT | COOKING | SANDVIK | FIRMDALE | LANCASTER | WILLIAMHILL | 購物 | اراسكو | |
| AM | MD | ART | HKT | OVH | AKDN | GGEE | PHOHL | APPLE | LILLY | TUSHU | GIVING | SOCCER | CORSICA | SCHMIDT | FOOTBALL | MARKETING | CONSTRUCTION | クラブド | التعليات | |
| AR | ME | AWS | HOT | PAY | ALLY | GMBH | PORN | ARCHI | LOANS | VEGAS | GLOBAL | SOCIAL | COUNTRY | SCHWARZ | FRONTIER | MARSHALLS | LPLFINANCIAL | ৴৴৴ | موريتانيا | |
| AT | MM | AXA | HOW | PET | AMEX | GOLD | POST | AUTOS | LOCUS | VIDEO | GOOGLE | STREAM | COUPONS | SCIENCE | GOODYEAR | MELBOURNE | SCHOLARSHIPS | 通販 | پاكستان | |
| AW | MN | BAR | IBM | PHD | ARAB | GOLF | PROD | BAIDU | LOTTE | VODKA | GRATIS | STUDIO | COURSES | SHIKSHA | GRAINGER | PANASONIC | VERSICHERUNG | भारत | بھارت | |
| AZ | MR | BBC | ICU | PID | ARMY | GOOG | PROF | BEATS | LOTTO | WALES | HEALTH | SUPPLY | CRICKET | SINGLES | PASSAGENS | MELBOURNE | INTERNATIONAL | भारत | بھارت | |
| BE | MX | BCG | INC | PIN | ASIA | GUGE | QPON | BIBLE | MEDIA | WATCH | HERMES | SUZUKI | CRUISES | STAPLES | HDFCBANK | PRAMERICA | LIFEINSURANCE | भारत | بھارت | |
| BG | MY | BET | ING | PNC | AUDI | GURU | READ | BINGO | MIAMI | WEIBO | HOCKEY | SYDNEY | DENTIST | STORAGE | WEIBO | RICHARDLI | WOLTERSKLUEWER | 网店 | اوططني | |
| BH | NC | BID | INK | PRO | ARMY | HAIR | REIT | BLACK | MONEY | WORKS | HOTELS | TAIPEI | DIGITAL | SUPPORT | HOLDINGS | SOLUTIONS | BANANAREPUBLIC | ৴৴৴ | البحرين | |
| BM | NF | BIO | INT | PRU | BAND | HAUS | RENT | BOATS | MOVIE | WORLD | HUGHES | TAOBAO | DOMAINS | SURGERY | STATEBANK | CANCERRESEARCH | BANANAREPUBLIC | 餐厅 | السعودية | |
| BN | NL | BIZ | IST | PUB | BANK | HDFC | REST | BUILD | MUSIC | XEROX | IMAMAT | TARGET | EXPOSED | SYSTEMS | INFINITY | STATEFARM | WEATHERCHANNEL | 网络 | السعودية | |
| BW | NZ | BMW | ITV | PWC | BBVA | HERE | RICH | CANON | NEXUS | ABARTH | INSURE | TENNIS | EXPRESS | TEMASEK | IPIRANGA | STOCKHOLM | AMERICANEXPRESS | 香港 | كوتونيك | |
| BY | OM | BOM | JCB | REB | BEER | HOST | ROOM | CARDS | NINJA | ABBOTT | INSURE | TENNIS | EXPRESS | TEMASEK | IPIRANGA | STOCKHOLM | AMERICANEXPRESS | 亚马逊 | همراه | |
| BZ | PE | BOO | JIO | REN | BEST | HSBC | RSVP | CHASE </td <td>NOKIA</td> <td>ABBVIE</td> <td>JOBURG</td> <td>TJMAXX</td> <td>FASHION</td> <td>THEATRE</td> <td>IPMORGAN</td> <td>VACATIONS</td> <td>SANDVIKCOROMANT</td> <td>诺基亚</td> <td>مليسيا</td> | NOKIA | ABBVIE | JOBURG | TJMAXX | FASHION | THEATRE | IPMORGAN | VACATIONS | SANDVIKCOROMANT | 诺基亚 | مليسيا | |
| CA | PL | BOT | JLL | RIL | BIKE | ICBC | SAFE | CHASE </td <td>NOKIA</td> <td>ABBVIE</td> <td>JOBURG</td> <td>TJMAXX</td> <td>FASHION</td> <td>THEATRE</td> <td>IPMORGAN</td> <td>VACATIONS</td> <td>SANDVIKCOROMANT</td> <td>诺基亚</td> <td>مليسيا</td> | NOKIA | ABBVIE | JOBURG | TJMAXX | FASHION | THEATRE | IPMORGAN | VACATIONS | SANDVIKCOROMANT | 诺基亚 | مليسيا | |
| CN | PM | BOX | JMP | RIO | BLOG | IEEE | SALE | CISCO | OSAKA | AGENCY | KINDER | TOYOTA | FERRERO | TOSHIBA | LIGHTING | MARRIOTT | ASSOCIATES | 飞利浦 | بيك | |
| CO | PT | BUY | JNJ | RIP | BLUE | IMDB | SARL | CITIC | PARIS | ALIPAY | KINDER | TOYOTA | FERRERO | TOSHIBA | LIGHTING | MARRIOTT | ASSOCIATES | 飞利浦 | عرب | |
| CR | PW | BZH | JOT | RUN | BOND | IMMO | SAVE | CLOUD | PARTS | ALIPAY | KINDER | TOYOTA | FERRERO | TOSHIBA | LIGHTING | MARRIOTT | ASSOCIATES | 飞利浦 | عرب | |
| CX | RE | CAB | JOY | SAS | BOOK | INFO | SAXO | COACH | PARTY | AMAZON | UNICOM | VIAJES | FITNESS | WATCHES | MEMORIAL | MCKINSEY | ASSOCIATES | 手机 | مصر | |
| DE | RO | CAL | KFH | SBI | BUZZ | ITAU | SEEK | CODES | PHONE | ARAMCO | LATINO | VIKING | FLIGHTS | WEATHER | MORTGAGE | BNPBBARIBAS | ASSOCIATES | 手机 | مصر | |
| DK | RS | CAM | KIA | SBS | CAFE | JEEP | SHAW | CYMRU | PIZZA | AUTHOR | LAWYER | VILLAS | FLORIST | WEBSITE | OBSERVER | BOEHRINGER | ASSOCIATES | 手机 | مصر | |
| DM | RU | CBA | KIM | SCB | CALL | JOBS | SHIA | DABUR | PLACE | BEAUTY | LOCKER | VIRGIN | FORSALE | WEDDING | PARTNERS | CONSULTING | ASSOCIATES | 手机 | مصر | |
| ES | RW | CBN | KPN | SEW | CAMP | JPRS | SHOP | DANCE | POKER | BERLIN | LONDON | VISION | FROGANS | WINNERS | PHARMACY | CREDITCARD | ASSOCIATES | 手机 | مصر | |
| ET | SA | CBS | KRD | SEX | CARE | KDDI | SHOW | DEALS | PRAXI | BOSTIX | LUXURY | VOTING | FUJITSU | WINNERS | PHARMACY | CREDITCARD | ASSOCIATES | 手机 | مصر | |
| EU | SB | CEO | LAT | SFR | CASA | KIDS | SILK | DELTA | PRESS | BOSTON | MAISON | VOYAGE | GALLERY | YAMAXUN | PLUMBING | EXTRASPACE | ASSOCIATES | 手机 | مصر | |
| FI | SC | CFD | LAW | SKI | CASE | KIWI | SINA | DRIVE | PRIME | BROKER | MAKEUP | VOYAGE | GALLERY | YAMAXUN | PLUMBING | EXTRASPACE | ASSOCIATES | 手机 | مصر | |
| FJ | SG | CPA | LDS | SOY | CASH | KPMG | SITE | DUBAI | PROMO | CAMERA | MARKET | WALTER | HAMBURG | ZUERICH | RELIANCE | HEALTHCARE | ASSOCIATES | 手机 | مصر | |
| FM | SH | DAD | LLC | SPA | CBRE | KRED | SKIN | EARTH | QUEST | CAREER | MATTEL | WEBCAM | HANGOUT | ABUDHABI | SAARLAND | IMMOBILIEN | ASSOCIATES | 手机 | مصر | |
| FO | SI | DAY | LLP | SRL | CERN | LAND | SNCF | EDEKA | REHAB | CASINO | MOBILE | YACHTS | HITACHI | AIRFORCE | SECURITY | INDUSTRIES | ASSOCIATES | 手机 | مصر | |
| FR | SK | DDS | LPL | STC | CHAT | LGBT | SOHU | EMAIL | REISE | CENTER | MONASH | HOLIDAY | AIRFORCE | SECURITY | INDUSTRIES | ASSOCIATES | 手机 | مصر | | |
| GD | SN | DEV | LTD | TAB | CITI | LIDL | SONG | EPSON | RICOH | CHROME | MORMON | ZAPPOS | HOTEL | ATTORNEY | SERVICES | MANAGEMENT | ASSOCIATES | 手机 | مصر | |
| GG | SS | DHL | MAP | TAX | CITY | LIFE | LIDL | SONG | EPSON | RICOH | CHROME | MORMON | ZAPPOS | HOTEL | ATTORNEY | SERVICES | MANAGEMENT | ASSOCIATES | 手机 | مصر |
| GI | SU | DNP | MBA | TCI | CLUB | LIKE | SPOT | FEDEX | RODEO | CHURCH | MOSCOW | ABOGADO | HYUNDAI | BARCLAYS | SHOWTIME | PROPERTIES | ASSOCIATES | 手机 | مصر | |
| GL | SX | DOG | MED | TDK | COOL | LIMO | STAR | FINAL | RUGBY | CLAIMS | MUTUAL | AGAKHAN | JEWELRY | BASEBALL | SOFTWARE | PRUDENTIAL | ASSOCIATES | 手机 | مصر | |
| GR | TF | DOT | MEN | TEL | COOP | LIVE | SURF | FOREX | SALON | ALIBABA | CLINIC | NAGUYA | KITCHEN | BOUTIQUE | STCGROUP | REALESTATE | ASSOCIATES | 手机 | مصر | |
| GS | TH | DTV | MIL | THD | CYOU | LOAN | TALK | FORUM | SEVEN | COFFEE | NATURA | ANDROID | KOMATSU | BRADESCO | SUPPLIES | REPUBLICAN | ASSOCIATES | 手机 | مصر | |
| GW | TL | DVR | MIT | TJX | DATA | LOFT | TAXI | GAMES | SHARP | CONDOS | ATHLETA | LANXESS | BROADWAY | BRUSSELS | TRAINING | RESTAURANT | ASSOCIATES | 手机 | مصر | |
| GY | TM | EAT | MLB | TOP | DATE | LOVE | TEAM | GIFTS | SHOES | COUPON | NOWRUZ | AUCTION | LASALLE | BRUSSELS | VENTURES | REPUBLICAN | ASSOCIATES | 手机 | مصر | |
| HK | TT | ECO | MLS | TRV | DCLK | LTDA | TECH | GIVES | SKYPE | CREDIT | OFFICE | AUDIBLE | LATROBE | BUILDERS | WOODSIDE | RESTAURANT | ASSOCIATES | 手机 | مصر | |
| HN | TW | ESQ | MMA | TUI | DEAL | LUXE | TEVA | GLASS | SLING | CRUISE | OLAYAN | NOWRUZ | AUCTION | LASALLE | BRUSSELS | VENTURES | ASSOCIATES | 手机 | مصر | |
| HR | TZ | FAN | MOE | TVS | DELL | MEET | TIPS | SMART | GLOBO | DATING | ONLINE | AVIANCA | LIMITED | CAPTETOWN | BUSINESS | UNIVERSITY | ASSOCIATES | 手机 | مصر | |
| HU | UA | FIT | MOI | UNO | DESI | MEME | TOWN | GMAIL | SMILE | DATSUN | OTSUKA | BANAMEX | LINCOLN | CATERING | CAPETOWN | VLAANDEREN | ASSOCIATES | 手机 | مصر | |
| IE | UG | FLY | MOV | UOL | DISH | MENU | TOYS | GREEN | SOLAR | DEALER | PFIZER | BENTLEY | MARKETS | CATHOLIC | ALFAROMEIO | LAANDEREN | ASSOCIATES | 手机 | مصر | |
| IL | US | FOO | MTN | UPS | DOCS | MINI | TUBE | GRIPPE | SPACE | DEGREE | PHOTOS | BENTLEY | MARKETS | CATHOLIC | ALFAROMEIO | LAANDEREN | ASSOCIATES | 手机 | مصر | |
| IN | UY | FOX | MTR | VET | DVAG | MINT | VIVA | GROUP | STADA | DENTAL | PHYSIO | BOOKING | NETBANK | CLEANING | AMSTERDAM | ACCOUNTANTS | ASSOCIATES | 手机 | مصر | |
| IO | UZ | FRL | NBA | VIG | FAGE | MOBI | VIVO | GUCCI | STORE | DESIGN | NETFLIX | BROTHER | NETFLIX | CLINIQUE | ANALYTICS | BARCLAYCARD | ASSOCIATES | 手机 | مصر | |
| IT | VC | FTR | NEC | VIN | FAIL | MODA | VOTE | GUIDE | STUDY | DIRECT | REALTY | BUGATTI | NETWORK | CLOTHING | AQUARELLE | BLOCKBUSTER | ASSOCIATES | 手机 | مصر | |
| JE | VG | FUN | NEW | VIP | FANS | MOTO | VOTO | HOMES | STYLE | DOCTOR | REISEN | CAPITAL | NEUSTAR | COMMBANK | DIRECTORY | CONTRACTORS | ASSOCIATES | 手机 | مصر | |
| JP | VN | FYI | NFL | WIN | FARM | NAVY | WANG | HONDA | SUCKS | DUNLOP | REPAIR | CARAVAN | OKINAWA | COMPUTER | EQUIPMENT | CREDITUNION | ASSOCIATES | 手机 | مصر | |
| KE | VU | GAP | NGO | WME | FAST | NEWS | WIEN | HORSE | TATAR | DURPONT | REPORT | CAREERS | OLDNAVY | DELIVERY | FINANCIAL | ENGINEERING | ASSOCIATES | 手机 | مصر | |
| KI | WF | GAY | NHK | WOW | FIAT | NICO | WIKI | HOUSE | TIRES | DURBAN | REVIEW | CAREERS | OLDNAVY | DELIVERY | FINANCIAL | ENGINEERING | ASSOCIATES | 手机 | مصر | |
| KR | WS | GDN | NOW | WTC | FIDO | NIKE | WINE | HYATT | TIROL | EMERCK | ROCHER | CHANNEL | CHARITY | DELOITTE | FIRESTONE | ENTERPRISES | ASSOCIATES | 手机 | مصر | |
| KW | YT | GEA | NRA | WTF | FILM | OLLO | WORK | IKANO | TIROL | EMERCK | ROCHER | CHANNEL | CHARITY | DELOITTE | FIRESTONE | ENTERPRISES | ASSOCIATES | 手机 | مصر | |
| LA | ZA | GLE | NTT | XIN | FIRE | OPEN | YOGA | IRISH | TMAIL | ENERGY | ROGERS | ENERGY | PHILIPS | DIAMONDS | FRENIUS | INVESTMENTS | ASSOCIATES | 手机 | مصر | |
| LC | AAA | GMO | NYC | XXX | FISH | PAGE | ZARA | JETZT | TMAIL | ENERGY | ROGERS | ENERGY | PHILIPS | DIAMONDS | FRENIUS | INVESTMENTS | ASSOCIATES | 手机 | مصر | |
| LT | ACO | GOO | ONE | XYZ | FLIR | PARS | ZERO | KOELN | TMAIL | ENERGY | ROGERS | ENERGY | PHILIPS | DIAMONDS | FRENIUS | INVESTMENTS | ASSOCIATES | 手机 | مصر | |
| LU | ADS | GOP | ONG | YOU | FORD | PCCW | ZONE | KYOTO | TORAY | FAMILY | SCHOOL | COMCAST | RECIPES | ENGINEER | HOMEDEPOT | PLAYSTATION | ASSOCIATES | 手机 | مصر | |

1149 TLDs in total
As of 7 June 2022
Source: TLD Apex History

Proposal for avoiding large outage at TLDs (1/3)

- At TLD side
 - Change the NSEC3 parameters to recommended value of nsec3-guidance ASAP prior or soon after the publication of nsec3-guidance BCP RFC
 - At least, iteration count to 0 and empty salt
 - Completion of changes is desirable within a half year after the BCP RFC publication

Proposal for avoiding large outage at TLDs (2/3)

- At validator (full resolver) side
 - Prepare a certain graceful period before changing the treatment of name resolution for iteration count larger than 0 to insecure or SERVFAIL
 - At least, prepare a half year graceful period after the BCP RFC publication
 - If willing to change to SERVFAIL, staged approach that change to insecure first for a certain period and then change to SERVFAIL is preferable

Proposal for avoiding large outage at TLDs (3/3)

- At DNS community side
 - Let have a global consensus regarding to a certain graceful period prior to validator side's changes
 - How about deciding a global target date?
 - I'm not sure if the next DNS Flag Day target and date are decided already, but this would be a good candidate, wouldn't it?

Past DNS Flag Day information is available at
<https://dnsflagday.net/2020/>

Your suggestions are
very welcome!