Are we ready for nsec3-guidance?

30 July 2022

DNS-OARC 38 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
  - Mainly focused on full resolver operators
- **Aiming smooth deployment of nsec3-guidance**

Key points of nsec3-guidance (1/3)

- Premise
  - nsec3-guidance indicates that using iteration count larger than 0 (> 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 (such as TLD)
  - 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 (such as public resolvers and ISP's 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*

"MAY" means "optional" and experienced resolver operators will employ the "option" prudently, but it is not sure

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 AD AF AG AM AR AT AW AZ BE BG BH BM BN BW BY BZ CA CN CO CR CX DE DK DM ES ET EU FI FJ FM FO FR GD GG GI GL GR GS GW GY HK HN HR HU IE IL IN IO IT JE JP KE KI KR KW LA LC LT LU

LV LY MA MC MD ME MM MN MR MX MY NC NF NL NZ OM PE PL PM PT PW RE RO RS RU RW SA SB SC SG SH SI SK SN SS SU SX TF TH TL TM TT TW UA UG US UY UZ VC VG VN VU WF WS YT ZA AAA ACO ADS AFL

AIG ANZ APP ART AWS AXA BAR BBC BCG BET BID BIO BIZ BMW BOM BOO BOT BOX BUY BZH CAB CAL CAM CBA CBN CBS CEO CFD CPA DAD DAY DDS DEV DHL DNP DOG DOT DTV DVR EAT ECO ESQ FAN FIT FLY FOO FOX FRL FTR FUN FYI GAP GAY GDN GEA GLE GMO GOO GOP GOT

GOV HBO HIV HKT HOT HOW IBM ICU INC ING INK INT IST ITV JCB JIO JLL JMP JNJ JOT JOY KFH KIA KIM KPN KRD LAT LAW LDS LLC LLP LPL LTD MAP MBA MED MEN MIL MIT MLB MLS MMA MOE MOI MOV MTN MTR NBA NEC NEW NFL NGO NHK NOW NRA NTT NYC ONE ONG ONL

OOO ORG OTT OVH PAY PET PHD PID PIN PNC PRO PRU PUB PWC RED REN RIL RIO RIP RUN SAS SBI SBS SCB SEW SEX SFR SKI SOY SPA SRL STC TAB TAX TCI TDK TEL THD TJX TOP TRV TUI TVS UNO UOL UPS VET VIG VIN VIP WIN WME WOW WTC WTF XIN XXX XYZ YOU ZIP

ABLE ADAC AERO AKDN ALLY AMEX ARAB ARMY ASIA AUDI BABY BAND BANK BBVA BEER BEST BIKE BLOG BLUE BOND BOOK BUZZ CAFE CALL CAMP CARE CASA CASE CASH CBRE CERN CHAT CITI CITY CLUB COOL COOP CYOU DATA DATE DCLK DEAL DELL DESI DISH DOCS DVAG FAGE FAIL FANS FARM FAST FIAT FIDO FILM FIRE FISH FLIR FORD FREE

FUND GBIZ GENT GGEE GMBH GOLD GOLF GOOG GUGE GURU HAIR HAUS HDFC HERE HOST HSBC ICBC IEEE IMDB IMMO INFO ITAU JEEP JOBS JPRS KDDI KIDS KIWI KPMG KRED LAND LGBT LIDL LIFE LIKE LIMO LIVE LOAN LOFT LOVE LTDA LUXE MEET MEME MENU MINI MINT MOBI MODA MOTO NAVY NEWS NICO NIKE OLLO OPEN PAGE PARS PCCW PING

PINK PLAY PLUS POHL PORN POST PROD PROF QPON READ REIT RENT REST RICH ROOM RSVP SAFE SALE SARL SAVE SAXO SEEK SHAW SHIA SHOP SHOW SILK SINA SITE SKIN SNCF SOHU SONG SONY SPOT STAR SURF TALK TAXI TEAM TECH TEVA TIPS TOWN TOYS TUBE VIVA VIVO VOTE VOTO WANG WIEN WIKI WINE WORK YOGA ZARA ZERO ZONE ACTOR

ADULT AETNA AMICA APPLE ARCHI AUTOS BAIDU BEATS BIBLE BINGO BLACK BOATS BUILD CANON CARDS CHASE CHEAP CISCO CITIC CLOUD COACH CODES CYMRU DABUR DANCE DEALS DELTA DRIVE DUBAI EARTH EDEKA EMAIL EPSON FAITH FEDEX FINAL FOREX FORUM GAMES GIFTS GIVES GLASS GLOBO GMAIL GREEN GRIPE GROUP GUCCI GUIDE HOMES HONDA HORSE HOUSE HYATT IKANO IRISH JETZT KOELN KYOTO LAMER

LEASE LEGAL LEXUS LILLY LOANS LOCUS LOTTE LOTTO MEDIA MIAMI MONEY MOVIE MUSIC NEXUS NINJA NOKIA NOWTV OSAKA OWNER PARIS PARTS PARTY PHONE PIZZA PLACE POKER PRAXI PRESS PRIME PROMO QUEST REHAB REISE RICOH ROCKS RODEO RUGBY SALON SEVEN SHARP SHOES SKYPE SLING SMART SMILE SOLAR SPACE STADA STORE STUDY STYLE SUCKS TATAR TIRES TIROL TMALL TODAY TOKYO TOOLS TORAY

TOTAL TOURS TRADE TUNES TUSHU VEGAS VIDEO VODKA WALES WATCH WEIBO WORKS WORLD XEROX ABARTH ABBOTT ABBVIE AFRICA AGENCY ALIPAY ALSACE AMAZON ARAMCO AUTHOR BEAUTY BERLIN BOSTIK BOSTON BROKER CAMERA CAREER CASINO CENTER CHROME CHURCH CIRCLE CLAIMS CLINIC COFFEE CONDOS COUPON CREDIT CRUISE DATING DATSUN DEALER DEGREE DENTAL DESIGN DIRECT DOCTOR DUNLOP DUPONT DURBAN EMERCK ENERGY ESTATE EVENTS EXPERT FAMILY

FLICKR FUTBOL GALLUP GARDEN GIVING GLOBAL GOOGLE GRATIS HEALTH HERMES HOCKEY HOTELS HUGHES IMAMAT INSURE INTUIT JOBURG KAUFEN KINDER KINDLE KOSHER LANCIA LATINO LAWYER LOCKER LONDON LUXURY MAISON MAKEUP MARKET MATTEL MOBILE MONASH MORMON MOSCOW MUSEUM MUTUAL NAGOYA NATURA NISSAN NOWRUZ OFFICE OLAYAN ONLINE OTSUKA PFIZER PHOTOS PHYSIO RACING REALTY REISEN REPAIR REPORT REVIEW ROCHER ROGERS RYUKYU SAFETY SAKURA SCHOOL

SCHULE SEARCH SECURE SELECT SOCCER SOCIAL STREAM STUDIO SUPPLY SUZUKI SYDNEY TAIPEI TAOBAO TARGET TENNIS TIENDA TJMAXX TKMAXX TOYOTA TRAVEL UNICOM VIAJES VIKING VILLAS VIRGIN VISION VOTING VOYAGE VUELOS WALTER WEBCAM YACHTS YANDEX ZAPPOS ABOGADO ACADEMY AGAKHAN ALIBABA ANDROID ATHLETA AUCTION AUDIBLE AUSPOST AVIANCA BANAMEX BENTLEY BESTBUY BOOKING BROTHER BUGATTI CAPITAL CARAVAN CAREERS CHANNEL CHARITY CHINTAI CITADEL COLLEGE COLOGNE COMCAST

COMPANY COMPARE CONTACT COOKING CORSICA COUNTRY COUPONS COURSES CRICKET CRUISES DENTIST DIGITAL DOMAINS EXPOSED EXPRESS FARMERS FASHION FERRARI FERRERO FINANCE FISHING FITNESS FLIGHTS FLORIST FORSALE FROGANS FUJITSU GALLERY GODADDY HAMBURG HANGOUT HITACHI HOLIDAY HOTELES HYUNDAI ISMAILI JEWELRY KITCHEN KOMATSU LANXESS LASALLE LATROBE LECLERC LIMITED LINCOLN MARKETS MONSTER NETBANK NETFLIX NETWORK NEUSTAR OKINAWA OLDNAVY ORGANIC ORIGINS PHILIPS PIONEER POLITIE REALTOR RECIPES

RENTALS REVIEWS SAMSUNG SANDVIK SCHMIDT SCHWARZ SCIENCE SHIKSHA SINGLES STAPLES STORAGE SUPPORT SURGERY SYSTEMS TEMASEK THEATER THEATRE TICKETS TOSHIBA TRADING WANGGOU WATCHES WEATHER WEBSITE WEDDING WINNERS XFINITY YAMAXUN YOUTUBE ZUERICH ABUDHABI AIRFORCE ALLSTATE ATTORNEY BARCLAYS BARGAINS BASEBALL BOUTIQUE BRADESCO BROADWAY BRUSSELS BUILDERS BUSINESS CAPETOWN CATERING CATHOLIC CIPRIANI CLEANING CLINIQUE CLOTHING COMMBANK COMPUTER DELIVERY DELOITTE DEMOCRAT DIAMONDS DISCOUNT DISCOVER DOWNLOAD ENGINEER

ETISALAT EXCHANGE FEEDBACK FIRMDALE FOOTBALL FRONTIER GOODYEAR GRAINGER GRAPHICS HDFCBANK HELSINKI HOLDINGS HOSPITAL INFINITI IPIRANGA ISTANBUL JPMORGAN LIGHTING MARRIOTT MASERATI MCKINSEY MEMORIAL MORTGAGE OBSERVER PARTNERS PHARMACY PICTURES PLUMBING REDSTONE RELIANCE SAARLAND SECURITY SERVICES SHOPPING SHOWTIME SOFTBANK SOFTWARE STCGROUP SUPPLIES TRAINING VENTURES WOODSIDE YOKOHAMA ALFAROMEO ALLFINANZ AMSTERDAM ANALYTICS AQUARELLE COMMUNITY DIRECTORY EDUCATION EQUIPMENT FINANCIAL FIRESTONE FRESENIUS FURNITURE GOLDPOINT HISAMITSU HOMEDEPOT HOMEGOODS

HOMESENSE INSTITUTE INSURANCE LANCASTER MARKETING MARSHALLS MELBOURNE PANASONIC PASSAGENS PRAMERICA RICHARDLI SOLUTIONS STATEBANK STATEFARM STOCKHOLM TRAVELERS VACATIONS YODOBASHI ACCOUNTANT APARTMENTS ASSOCIATES BASKETBALL BNPPARIBAS BOEHRINGER CONSULTING CREDITCARD CUISINELLA EXTRASPACE FOUNDATION HEALTHCARE IMMOBILIEN INDUSTRIES MANAGEMENT MITSUBISHI PROPERTIES PROTECTION PRUDENTIAL REALESTATE REPUBLICAN RESTAURANT SCHAEFFLER TECHNOLOGY UNIVERSITY VLAANDEREN VOLKSWAGEN ACCOUNTANTS BARCLAYCARD BLOCKBUSTER BRIDGESTONE CALVINKLEIN CONTRACTORS CREDITUNION ENGINEERING ENTERPRISES INVESTMENTS LAMBORGHINI MOTORCYCLES OLAYANGROUP PHOTOGRAPHY PLAYSTATION

PRODUCTIONS PROGRESSIVE REDUMBRELLA WILLIAMHILL CONSTRUCTION LPLFINANCIAL SCHOLARSHIPS VERSICHERUNG INTERNATIONAL LIFEINSURANCE WOLTERSKLUWER BANANAREPUBLIC CANCERRESEARCH WEATHERCHANNEL AMERICANEXPRESS SANDVIKCOROMANT TRAVELERSINSURANCE NORTHWESTERNMUTUAL セール 佛山 ಭಾರತ 慈善 集团 한국 ଭାରତ ভাৰত ভারত 八卦 公益 公司 网站 移动 我爱你 москва католик 联通 срб бг бел 时尚 微博 淡马锡 ファッション орг ストア アマゾン 삼성 சிங்கப்பூர் 商标 商店 商城 дети ею ポイント 新闻 家電 中信 中国 中國 娱乐

谷歌 భారత్ 電訊盈科 购物 クラウド ભારત 通販 भारतम् भारत भारोत 网店 संगठन 餐厅 网络 香港 亚马逊 诺基亚 食品 飞利浦 台湾 台灣 手机 政府 机构 组织机构 ไทย 招聘 рус рф ລາວ みんな グーグル ευ ελ 書籍 ഭാരതം ਭਾਰਤ 网址 天主教 游戏 vermögensberater vermögensberatung 企业 广东 இந்தியா հայ 新加坡 政务

ישראל موقع عمان ارامكو العليان اتصالات موريتانيا پاکستان بارت بهارت ابوظبي البحرين السعودية [illegible] كاثوليك همراه مليسيا شبكة بيتك عرب مصر

1149 TLDs in total
As of 9 July 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
  - Think carefully whether employing the “option”
  - 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?
    - Where can we discuss about it?

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

Your suggestions are very welcome!